W-8407L

Reference 2

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 November 2002 (21.11.2002)

PCT

(10) International Publication Number
WO 02/093877 A1

(51) International Patent Classification[7]: H04M 1/00, 3/00, 3/42, 11/10, H04B 1/38

(21) International Application Number: PCT/IB02/01550

(22) International Filing Date: 7 May 2002 (07.05.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/854,628 15 May 2001 (15.05.2001) US

(71) Applicants: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI). **NOKIA INC.** [US/US]; 6000 Connection Drive, Irving, TX 75039 (US).

(72) Inventors: **NYKÄNEN, Petri**; Lehdokkikatu 3, FIN-37120 Nokia (FI). **PALONIEMI, Jari**; Yliki-imingintie 169, FIN-90900 Kiiminki (FI). **KANGAS, Petri**; Pölkkytie 7A3, FIN-90800 Oulu (FI).

(74) Agent: **HOEL, John**; Morgan & Finnegan, LLP, 345 Park Avenue, New York, NY 10154 (US).

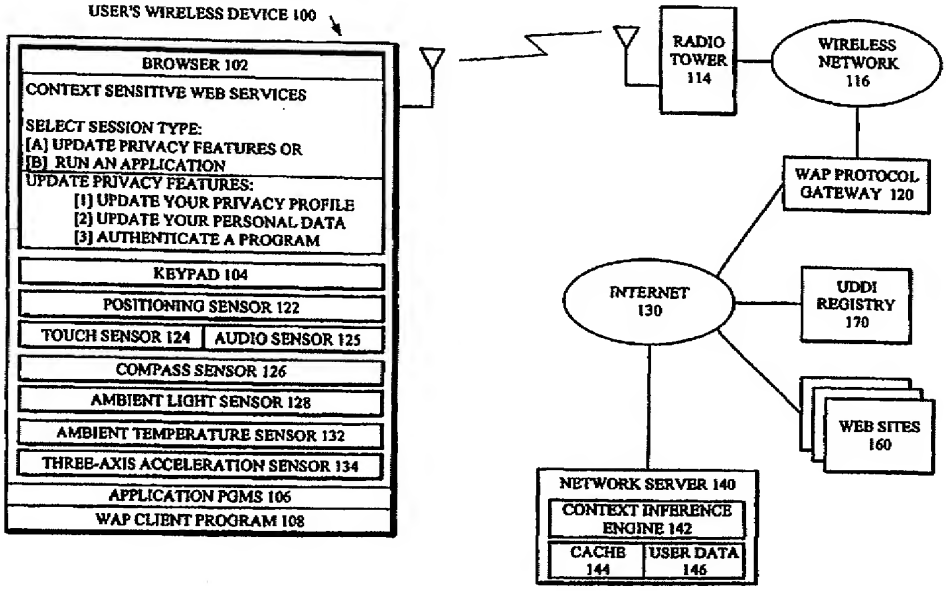
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: CONTEXT SENSITIVE WEB SERVICES



(57) Abstract: The context sensitive web services method enables a mobile phone or wireless device (100) to use context inference techniques to sense the user's environment and in response, to provide useful information to the user that is appropriate to the user's perceived environment. The method includes the steps of receiving sensor signals (122-134) characterizing a current environment of the wireless device (100); processing the sensor signals with a context inference engine (142); outputting a current context result from the processing by the context inference engine (142); and providing useful information to the user in response to the current context result.

WO 02/093877 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

CONTEXT SENSITIVE WEB SERVICES

This application claims priority to U.S. Application Serial No. 09/857,628, filed May 15, 2001, entitled, "Context Sensitive Web Services, which is incorporated herein by reference.

BACKGROUND OF THE INVENTION

Field of the Invention:

The invention disclosed broadly relates to methods for providing Internet services and more particularly relates to improvements in mobile device accessing of Internet services.

Background Art:

Mobile phones and wireless personal digital assistants (PDAs) are able to access the Internet using the Wireless Application Protocol (WAP). WAP-enabled wireless devices can now access Internet applications such as headline news, exchange rates, sports results, stock quotes, weather forecasts, multilingual phrase dictionaries, personal online calendars, online travel and banking services, or download distinctive ringing tones. Broadband wireless networks make it possible for WAP-enabled wireless devices to exchange multimedia messages that combine conventional text with much richer content types, such as photographs, images, voice clips, and video clips. WAP-enabled wireless devices can be used to pay bills online using the wireless device as a virtual wallet. WAP-enabled wireless devices can deliver useful and informative advertising and transaction services from online merchants. WAP-enabled wireless devices now also provide entertainment services, such as interactive adventure games, quizzes, and chess tournaments.

What is needed is the ability of a mobile phone or wireless PDA to use context inference techniques to sense the mobile user's environment and in response, to provide useful information to the user that is appropriate to the user's perceived environment. It would be even more useful to offload some of the computationally intensive computing necessary in context inference techniques, from the mobile user's wireless device to a server and to web sites on the Internet. It would be beneficial to maintain a personal

profile of the mobile user's personal preferences in an online server or web site. It would be important to provide the mobile user with the ability to control any access to the user's profile by the online server or web site.

SUMMARY OF THE INVENTION:

The context sensitive web services invention enables a mobile phone or wireless PDA to use context inference techniques to sense the user's environment and in response, to provide useful information to the user that is appropriate to the user's perceived environment.

One aspect of the invention is a method to enable a wireless device to provide useful information to its user that is appropriate to the device's current environment. The method includes the steps of receiving sensor signals characterizing a current environment of the wireless device; processing the sensor signals with a context inference engine; outputting a current context result from the processing by context inference engine; and providing useful information to the user in response to the current context result. The processing of the sensor signals with a context inference engine is embodied as programmed instructions executed within the user's wireless device. In another aspect of the invention, the processing of the sensor signals with a context inference engine is embodied as programmed instructions executed within a separate network server in response to signals from the user's wireless device. The server can access files from a web server, for selective forwarding to the user's wireless device. A personal profile of the user can be maintained by the server.

A further aspect of the invention provides user control of access by application programs to the user's private data. This can also include providing user control of access by application programs to the user's private data in the server. Still further, this can also include providing user control of access by application programs in a web server, to the user's private data.

Another aspect of the invention is providing the current context result to an application program in response to the user control and receiving the useful information from the application program. The invention enables the user to grant access permission to the application program to access the current context result. This can be performed in

the user's wireless device or in the network server. The network server can carry out the control of access by application programs in web servers, in response to a user privacy profile received from the user's wireless device.

DESCRIPTION OF THE FIGURES:

Figure 1 is a network diagram of the invention, showing an example relationship between the user's Wireless Application Protocol (WAP)-enabled portable wireless device, the WAP protocol gateway to the Internet, the network server, the Universal Description, Discovery and Integration (UDDI) registry, and a plurality of web sites.

Figure 1A shows the user's wireless device with the UPDATE PRIVACY FEATURES: sub-menu of the Context Sensitive Services menu, enabling the user to UPDATE YOUR PRIVACY PROFILE or UPDATE YOUR PERSONAL DATA.

Figure 1B shows the user's wireless device with the UPDATE PRIVACY FEATURES: sub-menu of the Context Sensitive Services menu, enabling the user to AUTHENTICATE A PROGRAM and REGISTER A PROGRAM.

Figures 1C and 1D show the user's wireless device with the RUN AN APPLICATION sub-menu of the Context Sensitive Services menu, enabling the user to RUN AN APPLICATION.

Figure 2 is a functional block diagram of the wireless device 100, showing its various components and programs.

Figure 2A is a functional block diagram of the wireless device 100, the server 140, and the web server 160, and their interaction when exchanging a metadata vector 138 and privacy control data 150.

Figure 3 is a network process flow diagram of the interaction of the wireless device 100, network server 140, and web server 160 when carrying out the determination of the current context of the wireless device 100.

Figure 4 is a functional block diagram of the network server 140, showing the memory storing the application services software programs needed to perform the operations of the invention.

DISCUSSION OF THE PREFERRED EMBODIMENT:

The context sensitive web services invention enables a mobile phone or wireless PDA to use context inference techniques to sense the user's environment and in response, to provide useful information to the user that is appropriate to the user's perceived environment. The invention offloads some of the computationally intensive computing necessary in context inference techniques, from the mobile user's wireless device to a server and to web sites on the Internet. The context sensitive web services invention maintains a personal profile of the mobile user's personal preferences in an online server or web site. The mobile user is provided with the ability to control access by application programs in the wireless device, to the user's private data. The context sensitive web services invention provide the mobile user with the ability to control any access to the user's profile by the online server or web site.

The mobile user's wireless device is equipped with a context inference engine for providing and awareness of the mobile user's context to application programs, including third party applications. Since the processing power and storage capacity is limited in typical wireless devices, the computational load and storage requirements of the context inference engine are distributed to a context inference server capable of processing the context data. The invention enables the mobile user to control which application programs in the wireless device are granted access to the user's private context information. A privacy control block in the wireless device grants or revokes access by application programs to the private context information, based on the mobile user's preferences stored in a privacy profile. The same privacy control and privacy profile is extended to the context inference server, thereby enabling the extension of the user's privacy control to any web server connected to the context inference server. The invention thus enables building an infrastructure for context sensitive applications and services within the wireless device and the server, while providing to the mobile user control over the privacy user's context information.

The invention is applied to wireless telephones and wireless personal digital assistants (PDAs) implementing the Wireless Application Protocol (WAP) standard. Figure 1 is a network diagram of an embodiment of the invention, showing an example relationship between the user's Wireless Application Protocol (WAP)-enabled portable wireless device 100, a WAP protocol gateway 120, and the server 140. The user's WAP-enabled portable wireless device 100 can be a wireless mobile phone, pager, two-way

radio, smartphone, personal communicator, or the like. The user's WAP-enabled portable wireless device 100 accesses a small file called a deck which is composed of several smaller pages called cards which are small enough to fit into the display area of the device's microbrowser 102. The small size of the microbrowser 102 and the small file sizes accommodate the low memory constraints of the portable wireless device 100 and the low-bandwidth constraints of a wireless network 116. The cards are written in the Wireless Markup Language (WML) which is specifically devised for small screens and one-hand navigation without a keyboard. The WML language is scaleable from two-line text displays on the microbrowser 102 of a cellular telephone, up through large LCD screens found on smart phones and personal communicators. The cards written in the WML language can include programs written in WMLScript, which is similar to JavaScript, but makes minimal demands on memory and CPU power of the device 100 because it does not contain many of the unnecessary functions found in other scripting languages.

The Nokia WAP Client Version 2.0 is a software product containing the components necessary to implement the WAP client 108 on the wireless device 100. These components include a Wireless Markup Language (WML) Browser, WMLScript engine, Push Subsystem, and Wireless Protocol Stack. The Nokia WAP Client is a source-code product that can port and integrate into wireless devices such as mobile phones and wireless PDAs. Application programs 106 stored in the wireless device 100 interact with the WAP Client 108 to implement a variety of communications applications. Details of the Nokia WAP Client Version 2.0 can be found in the online paper: Nokia WAP Client Version 2.0, Product Overview, Nokia Internet Communications, 2000, www.nokia.com/corporate/wap.

The WAP Client 108 includes the Wireless Public Key infrastructure (PKI) feature, providing the infrastructure and the procedures required for authentication and digital signatures for servers and mobile clients. Wireless PKI is a certificate-based system that utilizes public/private key pairs associated with each party involved in a mobile transaction. Wireless Identity Module (WIM) is a security token feature of the WAP Client 108, which includes security features, such as the public and private keys and service certificates, needed for user authentication and digital signatures. Additionally, it has the ability to perform cryptographic operations to encrypt and decrypt messages.

The wireless device 100 of Figure 1 also has a plurality of sensors for sensing the mobile user's ambient conditions. The sensors shown include POSITIONING SENSOR 122, TOUCH SENSOR 124, AUDIO SENSOR 125, COMPASS SENSOR 126, AMBIENT LIGHT SENSOR 128, AMBIENT TEMPERATURE SENSOR 132, and THREE-AXIS ACCELERATION SENSOR 134. The audio sensor 125 can be a microphone, for example, which can detect speech or environmental sounds. The positioning sensor can be, for example, a GPS receiver integrated in the device. The positioning sensor can also be, for example, a radio beacon triangulation sensor that determines the location of the wireless device by means of a network of radio beacons, base stations, or access points, as is described for example, in Nokia European patent EP 0 767 594 A2, entitled "Mobile Station Positioning System". These sensors provide inputs which are sampled by the wireless device 100 to infer a current context, as will be described below.

The WAP protocol gateway 120 links the Internet 130 and the wireless network 116. The WAP protocol gateway 120 includes the Wireless Public Key infrastructure (PKI) feature to help provide a secure Internet connection to the wireless device 100. The WAP protocol gateway 120 enables the WAP-enabled wireless device 100 to access Internet applications such as headline news, exchange rates, sports results, stock quotes, online travel and banking services, or to download distinctive ringing tones.

The user's WAP-enabled portable wireless device 100 communicates with the radio tower 114 and can exchange messages for distances up to several kilometers. The types of wireless networks 116 supported by the WAP standard include Cellular Digital Packet Data (CDPD), Code-Division Multiple Access (CDMA), Global System for Mobile Communications (GSM), Time Division Multiple Access (TDMA), GPRS, 3G-Broadband, and the like.

The overall process of communication between the user's WAP-enabled wireless device (the client) 100, through the WAP protocol gateway 120, to the server 140 resembles the way Web pages are served on the Internet using the HyperText Transfer Protocol (HTTP) or World Wide Web protocol:

[1] The user presses a phone key on the user's device 100 related to the Uniform Resource Locator (URL) of the server 140.

[2] The user's device 100 sends the URL, via the radio tower 114 and the wireless network 116, to the gateway 120 using WAP protocols.

[3] The gateway 120 translates the WAP request into an HTTP request and sends it over the Internet 130 to the server 140, via Transmission Control Protocol/ Internet Protocol (TCP/IP) interfaces.

[4] The server 140 handles the request just like any other HTTP request received over the Internet. The server 140 either returns a WML deck or a HyperText Markup Language (HTML) page back to the gateway 120 using standard server programs written, for example in Common Gateway Interface (CGI) programs, Java servlets, or the like.

[5] The gateway 120 receives the response from the server 140 on behalf of the user's device 100. If the response is an HTML page, it gets transcoded into WML if necessary. Then the WML and WMLScript coding is encoded into a byte code that is then sent to the user's device 100.

[6] The user's device 100 receives the response in the WML byte code and displays the first card in the deck on the microbrowser 102 to the user.

In Figure 1, the protocol gateway 120 includes a WAP protocol stack organized into five different layers. An application layer is the wireless application environment, which executes portable applications and services. A session layer is the wireless session protocol, which supplies methods for the organized exchange of content between client/server applications. A transaction layer is the wireless transaction protocol, which provides methods for performing reliable transactions. A security layer is the wireless transport layer security, which provides authentication, privacy, and secure connections between applications. The transport layer is the wireless datagram protocol, which shelters the upper layers from the unique requirements of the diverse wireless network protocols, such as CDPD, CDMA, GSM, etc. Additional information about the WAP standard and the WAP protocol stack can be found in the book by Charles Arehart, et al. entitled, "Professional WAP", published by Wrox Press Ltd., 2000 (ISBN 1-861004-04-1).

In Figure 1, the user's portable wireless device 100 includes the microbrowser 102 displays the Context Sensitive Services menu, to enable the user to navigate through the cards being displayed and to select options that are programmed by the application

programs 106. The user's device 100 also includes the WAP client program 108 which has been previously discussed.

The Context Sensitive Services menu displayed by the microbrowser 102 in Figure 1 is rendered by the WAP client program 108 under the control of the application programs 106, which are shown in Figures 2 and 2A. The user can select the session type with Context Sensitive Services menu, either [A] UPDATE PRIVACY FEATURES or [B] RUN AN APPLICATION. If the UPDATE PRIVACY FEATURES session type is selected by the user, the Context Sensitive Services menu of Figure 1 then presents to the user the UPDATE PRIVACY FEATURES sub-menu from which the user can select the following options:

[A] UPDATE PRIVACY FEATURES:
[1] UPDATE YOUR PRIVACY PROFILE
[2] UPDATE YOUR PERSONAL DATA
[3] AUTHENTICATE A PROGRAM

Option [1] of UPDATE YOUR PRIVACY PROFILE, leads to a second sub-menu shown in Figure 1A, which has the following options:

[1] UPDATE YOUR PRIVACY PROFILE
[a] Add a local program to permissions list
[b] Remove a local program from list
[c] Add a server program to permissions list
[d] Remove a server program from list
[e] Add a network program to permissions list
[f] Remove a network program from list.

Option [2] of UPDATE YOUR PERSONAL DATA, leads to a another sub-menu shown in Figure 1A, which has the following options:

[2] UPDATE YOUR PERSONAL DATA
[a] Update server database
[b] Update network database.

Option [3] of AUTHENTICATE A PROGRAM, leads to a another sub-menu shown in Figure 1B, which has the following options:

[3] AUTHENTICATE A PROGRAM
[a] Request program's public key certificate
[b] Verify certificate signatures

[c] Verify validity time
[d] Verify revocation status
[e] Check if certificate authority on trust list
[f] Flag program as authenticated.

The AUTHENTICATE A PROGRAM option calls the privacy control 150 of the wireless device 100 in Figure 2. If an application program A, B, X, or Y has been verified for its acceptability by a trusted authority, then the trusted authority will have issued a digital certificate on a message authentication code (MAC) it has computed for the application program, which can be checked by the privacy control 150. As long as the privacy control 150 trusts the trusted authority issuing the digital certificate, authentication of the application program is straight forward.

Once the mobile user has verified the program's digital certificate and is satisfied that the application program will not subvert the integrity or security of the user's private data, the user can register the program. Registration is the granting by the user of access permission to the program, to access the current context of the user's wireless device and/or to access other portions of the user's private data. There are several levels of permission that can be granted by the user in two categories, [a] when can the accesses take place and [b] what data can be accessed.

Option [4] of REGISTER A PROGRAM, leads to a another sub-menu shown in Figure 1B, which has the following options:

[4] REGISTER A PROGRAM
[a] When can the accesses take place
[b] What data can be accessed

For the first category of [a] when can the accesses take place, the highest level of permission in this category is that access can occur anytime and without notice. The lowest level of permission in this category is that access can only occur at specified times or under specified conditions, and only after notice to the user and specific authorization by the user. For the second category of [b] what data can be accessed, the highest level of permission in this category is to access unlimited datasets in the user's private data, including current context information, personal data entered by the user, the user's Internet usage history data, the user's Internet cookie data, and the user's application program usage data. The lowest level of permission in this category is that access of any data can

only occur after notice to the user and specific authorization by the user. The user can configure any levels of permission in between the highest and lowest and make that the basis for the registration. The user can include the terms of registration in a digital certificate signed by the user and appended to the application program. This registration certificate can be presented by the program to the privacy control 150 prior to a proposed access event, the privacy control 150 to automatically verify the registration status of the program. The registration certificate can be constructed as follows.

The privacy control 150 can compute a message authentication code (MAC) and its own digital signature and append it as a certificate to an acceptable application program A, B, X, or Y. The privacy control 150 can include the terms of registration in the digital certificate. Then when the program requests access to the user's private data, the privacy control 150 can automatically check the MAC and its own digital signature to verify that the program has not been changed and the privacy control 150 can also automatically verify the registration status of the program. This is achieved by the privacy control 150 computing a hash value for the entire application program A, B, X, or Y (or some portion of it) and the terms of registration, and then forming a message authentication code (MAC) from the hash value. The privacy control 150 then uses its PKI private key to digitally sign the message authentication code (MAC). The terms of the registration, the MAC and the privacy control's digital signature are appended to the application program A, B, X, or Y as a registration certificate.

Then, whenever the application program A, B, X, or Y requests access to the user's context data or private data, the privacy control 150 will require the application program to present the registration certificate so that the privacy control 150 can check that the presented MAC compares with a computed MAC and that the presented digital signature is genuine. The privacy control 150 can then automatically grant access permission to the application program, in accordance with the terms of the registration.

Methods to generate and evaluate message authentication codes to insure the integrity of data are described in the book by Stephen Thomas entitled "SSL and TLS", published by John Wiley and Sons, 2000. Two example algorithms for message authentication are RSA's Message Digest (MD5) and the Secure Hash Algorithm (SHA),

both of which are described in the book by Stephen Thomas. Another reference that goes into greater detail in its discussion of data integrity methods is the book by Bruce Schneier entitled "Applied Cryptography - 2nd Edition" published by John Wiley and Sons, 1996. Methods to generate and evaluate digital signatures to insure the source of the digital program are described in the book by Richard E. Smith entitled "Internet Cryptography", published by Addison Wesley, 1997.

What has been described here for the privacy control 150 in the wireless device 100, is equally applicable to the privacy control 164 in the network server 140 of Figure 2A. The privacy control 164 in the network server 140 can compute the message authentication code (MAC) and its own digital signature and append it, with the terms of the registration, as a registration certificate to an acceptable application program in the web server 160. Privacy control 164 has a cached copy 144 of the Privacy Profile 152 of the wireless device 100. This enables automatically processing the privacy check in the network Server 140 for access requests from web server 160. When the application program in the web server 160 requests access to the user's private data in the network server 140 or in the wireless device 100, the privacy control 164 in the network server 140 will require the application program in the web server 160 to present the registration certificate so that it can check the MAC and its own digital signature to verify that the application program has not been changed. The privacy control 164 can then automatically grant access permission to the application program in the web server 160, in accordance with the terms of the registration.

If the [B] RUN AN APPLICATION session type is selected by the user, the Context Sensitive Services menu of Figure 1C then presents to the user the RUN AN APPLICATION sub-menu from which the user can select the following options:

[1] MESSAGING
[a] exchange multimedia messages

[2] MOBILE COMMERCE
[a] personal online calendar
[b] exchange rates
[c] banking services
[d] pay bills online using virtual wallet
[e] useful and informative advertising

[f] online merchant transaction services

The Context Sensitive Services menu of Figure 1D presents to the user the RUN AN APPLICATION sub-menu from which the user can select the following options:

[3] ENTERTAINMENT
[a] headline news
[b] sports results
[c] stock quotes
[d] weather forecasts
[e] multilingual phrase dictionaries
[f] online travel
[g] download distinctive ringing tones
[h] interactive games

The RUN AN APPLICATION option calls one of the application programs A, B, X, or Y of the wireless device 100 in Figure 2.

Figure 2 is a functional block diagram of the wireless device 100, showing its various components and programs. The wireless device 100 has context sensitive applications A, B, X, and Y, either downloaded, or in firmware. The wireless device 100 does not need to utilize external functionality in the network for the initial sampling and digitization of the sensor inputs. The sampled and digitized values of the sensor inputs are POSITIONING METADATA 122', TOUCH METADATA 124', AUDIO METADATA 125', COMPASS METADATA 126', AMBIENT LIGHT METADATA 128', AMBIENT TEMPERATURE METADATA 132', and THREE-AXIS ACCELERATION METADATA 134'. The sampled and digitized values of the sensor inputs are loaded into a metadata vector 138.

Figure 2 shows the memory 202 of the wireless device 100, connected by the bus 204 to the keypad 104, the radio 206, the sensor interface 208, the central processor 210, and the display 212. The memory 202 stores programs which are sequences of executable instructions which, when executed by the processor 210, carry out the methods of the invention. The memory 202 stores the WAP client program 108, the context inference engine 136, the privacy control 150, the privacy profile 152, the context aware API 154, the motion/gesture API 156, the location API 158, and other APIs 162. The context inference engine 136 processes the metadata vector 138 to produce the current context.

Application programs 106 stored in the memory 202 include the application programs A and B which are part of the software system SS1, and the application programs X and Y which are contained in the execution environment "Exec. Env."

If sufficient computational power and storage capacity are available in the wireless device 100, further processing of the metadata vector 138 can take place in the context inference engine 136, toward the objective of producing the result of an inferred current context. However, if at some point in the computation, the context inference engine 136 needs the processing power or storage capacity available at the network server 140, the metadata vector 138 is sent from the wireless device 100 to the context inference engine 142 in the network server 140 of Figure 2A. The context inference engine 142 in the network server 140 can perform the required processing on the metadata vector 138 and then return it to the context inference engine 136 in the wireless device 100 for completion of the an inferred current context result. Alternately, the context inference engine 142 in the network server 140 can complete the required processing and then return the resultant inferred current context to the wireless device 100.

Figure 2 shows the architecture of a wireless device with support for context awareness. The context awareness is built on top of sensory information received from various types of sensors physically located in the handset shown in Figure 1. The sensors shown include POSITIONING SENSOR 122, TOUCH SENSOR 124, AUDIO SENSOR 125, COMPASS SENSOR 126, AMBIENT LIGHT SENSOR 128, AMBIENT TEMPERATURE SENSOR 132, and THREE-AXIS ACCELERATION SENSOR 134. The sensors can also be located in accessory-like phone covers or in a wireless accessory such as a Bluetooth enabled device. The sensors may also be located in the environment such as in the user's rooms or vehicles. Also the time duration of use of a phone and other available information can be used along with sensor data in context awareness services.

Figure 2 shows sensor data received from the sensors 122, 124, 125, 126, 128, 132, and 134 is processed by Context Inference Engine 136. The application programs A, B, X, or Y running in the wireless device 100, may optionally provide application data to the context inference engine 136, along with their request for current context. The context inference engine 136 can optionally process the sensor signals and the application data to

produce the current context. The context inference engine 136 then feeds the current context through various APIs 154, 156, 158, and 162 to application programs A, B, X, and Y. The application programs may register themselves at the Application Programming Interface 154 to receive current context or changes in the context. This enables context sensitivity in the application programs.

Figure 2 shows "native" application programs A and B which are executed in a first software system SS1 of the wireless device 100. The term "Software System" is used here for any environment with execution capability. This first software system may be proprietary or based on a commercially available real-time operating system, such as NOS, ISA, EPOC, JAVA, or WAP. Third party application programs X and are executed within an execution environment. This execution environment may limit the system capabilities available for the application programs, such as access to APIs (fixed, not dynamic behavior).

Figure 2 shows the mobile user's privacy control feature. The privacy control feature enables the user to designate which application programs are granted access to the context awareness APIs 154 to utilize the current context information produced by the context inference engine 136. All requests or registrations by application programs A, B, X, and Y to have access to the Context Inference Engine 136, must first go through the Privacy Control block 150. Privacy Control block 150 uses the user's security data check stored in the Privacy Profile 152 to grant access rights to the requesting application programs. The user controls the granting of access rights by means of the user's security data input by the user through the user interface. The user's security data includes permissions list 155, Public Key Infrastructure (PKI) certificates 157, PKI trusted authority trust list 159, and flags set by the user for those application programs that have been authenticated by the PKI procedures, data set 161. The user can update the user's security data with the UPDATE PRIVACY FEATURES menu displayed by the wireless device 100 shown in Figures 1A and 1B. Access might be granted to an application program based on its digital signature, which is a part of the system applications, or other means known in the art. It is also possible to provide a separate system-wide Privacy User Interface to the privacy control 150, which can be employed by the mobile user to set the privacy policies and to alert the mobile user that an application program is attempting to

register to receive the user's private context awareness information. The privacy control 150 and Privacy Profile 152 enable the mobile user to grant, deny, or revoke access, to grant access for a limited time, or to require an application program to always request registration before the user grants access.

In Figure 2, the Context Inference Engine 136 in the wireless device 100 makes inferences from all the sensor inputs based on where the wireless device is located by the mobile user. For instance the inferred current context of the device 100 may be "IN THE USER'S POCKET", when a certain set of sensors input a specific combination of signals having a specific value range. As an example, the resulting inference of the current context by the Context Interference Engine 136 could be expressed in XML language format as follows:

<Context Inference Engine in Device>

<device placement> pocket </ device placement>

<User Interface state> sleep mode </User Interface state>

< device location> in elevator 5 building 1 floor 2</ device location>

<API active actions> meeting starting on floor 3 room 322 </API active actions>

</Context Inference Engine in Device >

The Context Inference Engine 136 in the wireless device 100 can perform the context inference process with any of several methods. Different input information from the sensors can be weighted according to their relative value of importance appropriate for each environment condition or situation to be analyzed. Each sensor has it's own weight value. Alternatively, the weight values for each sensor for each environment condition can be learned from training sessions using, for example artificial neural networks (ANNs), self-organizing maps (SOMs), decision trees, fuzzy rule-based systems, or model-based systems such as Hidden Markov Modeling (HMM). Combinations of two or more of the alternate methods can be used, depending on the application.

The Context Inference Engine 136 can continuously adapt its weights through adaptive and continuous learning methods, where the user teaches the wireless device 100 new environment conditions and names them. Hidden Markov Modeling (HMM) can be

used, for example, to implement an adaptive and continuous learning method for the Context Inference Engine 136. Alternately, the wireless device 100 can be programmed to spontaneously recognize a changed scene by comparing it with known scenes. The user can teach the wireless device new environmental conditions and name them, using the adaptive and automatic learning capability of neural networks. Adaptive and continuous learning methods are computationally intensive and are appropriate candidates to place on the network server 140, which assists the wireless device 100, as discussed below.

The field of context inference has applied the principles of automated pattern recognition to processing diverse types sensor inputs. Speech recognition has been applied to processing speech signals and handwriting recognition has been applied to processing hand force and accelerometer signals. In the field of robotics, image recognition has been applied to processing digitized still and motion images, mechanical location recognition has been applied to processing laser and sonar range finder signals, and mechanical motion recognition to has been applied to processing inertial, acceleration, and heading signals. In the field of prosthetic devices, touch recognition has been applied to processing tactile sensor signals. In the field of medicine, automated diagnostic programs recognize various pathologies by processing bioelectric field signals, as well as the more traditional pulse, respiration rate, and body temperature signals. These diverse sensor signal recognition processes have the common feature that an initial training stage is conducted where sampled signals are equated with a statistical model for those signals.

The principles of automated pattern recognition for these diverse sensor inputs are exemplified by the techniques for recognizing speech patterns. A common technique used in speech recognition is Hidden Markov Modeling (HMM). The term "Hidden" refers to the probabilistic and not directly observable events which underlie a speech signal. HMM speech recognition systems typically use realizations of phonemes which are statistical models of phonetic segments having parameters that are estimated from a set of training examples. Models of words are made by chaining or linking appropriate statistical models of phonetic segments. The statistical models serve as standards which are to be matched with the unknown voice signals to be recognized.

Recognition of unknown voice signals requires sampling and digitizing the speaker's spoken phonemes. These digitized phonemes are then processed into metadata. The metadata is then compared with the standard statistical models of phonemes. The most likely matches are then the inferred speech recognition result.

Recognition consists of finding the most likely path through the set of word models for the input speech signal. HMM speech recognition decoding systems first need to be trained through an iterative process. The system must be exposed to training examples or words of a particular speaker's voice. A training word is analyzed to generate a framed sequence of acoustic parameters or statistical models. A valid or "good" recognition occurs when the most likely path through the set of word models for the training word results in recognizing the correct training word.

Some useful references discussing the principles of Hidden Markov Models are:

Rabiner, L. R., "A tutorial on hidden Markov models and selected applications in speech recognition", Proceedings of the IEEE, volume 77, number 2, 1989, pages 257-286.

Rabiner, L. R. and Juang, B. H., "An introduction to hidden Markov models", IEEE ASSP Magazine, January 1986, pages 4-15.

Fraser, Andrew M. and Dimitriadis, Alexis, "Forecasting Probability Densities by Using Hidden Markov Models with Mixed States", Time Series Prediction: Forecasting the Future and Understanding the Past, Addison-Wesley, editor Weigend, Andreas S. and Gershenfeld, Neil A., 1994.

Charniak, Eugene, Statistical Language Learning, MIT Press, Cambridge, Massachusetts, 1993.

To illustrate how Hidden Markov Modeling (HMM) can be extended beyond speech recognition, an example is given here for touch recognition. In the training stage for touch recognition, tactile sensor signals are input from touching a tactile transducer to a rough texture, such as for example sandpaper. The tactile sensor signals are transformed into a statistical model of the input signal. The statistical model is stored as a standard in a computer memory under the handle "rough_texture". To expand the range of sensor signals that are included in the model for "rough_texture", several training

sessions can be conducted, each with a different direction or pressure for touching the sandpaper, resulting in several different samples of the statistical model. The set of samples of the statistical model are stored as a standard under the handle "rough_texture". Other training sessions are conducted with a smooth texture, such as glass. The tactile sensor signals input from touching the tactile transducer to the smooth texture are transformed into a statistical model of the input signal and stored as a standard under the handle "smooth_texture". Later, in the recognition mode, an unknown object is touched by the tactile transducer resulting in a sample tactile sensor signal. Recognition of unknown touch signals requires sampling and digitizing the touch transducer's signals. These digitized sensor signals are then processed into metadata. The metadata is then compared with the standard statistical models of "rough_texture" and "smooth_texture". The most likely match is then the inferred touch recognition result.

Combinations of two or more types of sensors can have their signals combined into an input metadata vector that characterizes a composite sampling event. The composite sampling event can be recognized using the principles of Hidden Markov Modeling (HMM). An example composite sampling event can be the state of the health and fatigue of the user of a wireless device 100. For example, a wireless device 100 can be equipped with a tactile transducer which outputs tactile sensor signals in response to the hand force and pulse rate of the user who is gripping the wireless device 100. The wireless device 100 can be equipped with a temperature sensor which outputs body temperature signals in response to the user gripping the wireless device 100. Hidden Markov Modeling (HMM) can be used to recognize a force/temperature input metadata vector that characterizes the combination of the hand force and the temperature sensor signals resulting from a sampling event. A composite sampling event in this example can have an extended duration so that the force sensor can transduce the pulse rate of the user over a period of time.

In the training stage, the tactile sensor signals and the force sensor signals are output while the user is in a condition of good health and resting normally. The tactile sensor signals and the force sensor signals are combined into a force/temperature input metadata vector which is transformed into a statistical model of the input signals. The statistical model is stored as a standard in the computer memory of the wireless device

100 under the handle "good_health_ resting_normally". Other training sessions are conducted with the user in different states of health and fatigue. For example, the user may be training the wireless device 100 while working late at night at the office. The tactile sensor signals and the force sensor signals resulting from holding the wireless device 100, are combined into a force/temperature input metadata vector for the user in the condition of being in good health but fatigued. The force/temperature input metadata vector is transformed into a statistical model of the input signals and stored as a standard under the handle "good_health_ fatigued".

Later, in the recognition mode, as the user holds the wireless device 100, the tactile sensor signals and the force sensor signals are sampled. The Health/Fatigue_State recognition consists of sampling and digitizing the touch transducer's signals. These digitized sensor signals are then processed into a metadata vector. The metadata vector is then compared with the standard statistical models of handle "good_health_ resting_normally" and "good_health_ fatigued". The most likely match is then the inferred touch recognition result.

In accordance with the invention, this recognition result can be used by a health maintenance application program in the wireless device 100, to provide useful and appropriate information to the user. For example, a health maintenance program can process the recognition result, and in response, signal an alarm to the user and provide suggestions for medications to palliate the sensed fatigue. One problem with automatic recognition programs is that they are either relatively large or they call databases that are relatively large in comparison to the memory capacity of the wireless device 100.

Another aspect of the invention is the recognition result can be used by a supplementary application program in a remote server, to provide additional and more detailed useful and appropriate information to the user. For example, the server can access a large database of suggestions for medications to palliate the sensed fatigue of the user. The results of the search of the database can be returned to the wireless device 100. The server can also maintain a personal profile of the user's characteristics and preferences and it can use that profile in automatically formulate its query to the database. For example, the user's drug allergies can be stored in the server's database, to insure that

recommendations are not made that will result in an allergic reaction by the user to the suggested medication.

Figure 2A is a functional block diagram of the wireless device 100, the server 140, and the web server 160, and their interaction when exchanging the metadata vector 138 and the privacy control data 150'. These exchanges are bulk encrypted with a symmetric session key, such as a Data Encryption Standard (DES) key, to protect the privacy of the data. To insure the integrity of the metadata vector 138 and the privacy control data 150', a message authentication code (MAC) can be computed and appended to the data, as described in the above referenced book by Stephen Thomas entitled "SSL and TLS", published by John Wiley and Sons, 2000. To insure that the source of the metadata vector 138 and the privacy control data 150' cannot be repudiated, a digital signature can be appended to the data, as described in the above referenced book by Richard E. Smith entitled "Internet Cryptography", published by Addison Wesley, 1997.

Figure 2A shows the scope of the distributed context awareness implementation. The wireless device 100 has context sensitive applications A, B, X, and Y either downloaded or in firmware. The wireless device 100 may locally preprocess part of the context information in the metadata vector 138 before sending it to the context inference engine 142 in the network server 140 which is capable of processing the data and responding back with the resulting current context. The wireless device 100 may run application programs that require accessing the web service server 160 to provide context sensitive services to the mobile user.

Figure 2A shows how processing of sensor data from the sensors in the wireless device 100, can be distributed between the wireless device and the network server 140. The operation in Figure 2A is as follows:

1. The sensors continuously provide the sensor data to the Context Inference Engine 136 in the wireless device 100.

2. An application program that utilizes the context awareness APIs 154 may request the latest context information, or the application program may be registered to receive any changes to specific context information.

3. The Context Inference Engine 136 securely contacts the Context Inference Engine 142 of the network server 140 and sends the metadata vector 138 to the server 140. Depending on the sensors and the implementation details, Context Inference Engine 136 may preprocess part of the sensor data in the metadata vector 138 prior to sending it. Depending on the sensors and the interval for processing, there may be virtual connection open between Context Inference Engine 136 and Context Inference Engine 142 for frequent data exchanges. Context Inference Engine 142 at the network server 140, has the processing power and memory capacity to handle computationally intensive and/or memory intensive processing of the preprocessed sensor data in the metadata vector 138 to produce the current context result information.

4. Context Inference Engine 142 at the network server 140 may utilize local user information (history information, customer details) stored in the user database 146 for making a more accurate determination of the mobile user's current context.

5. Context Inference Engine 142 at the network server 140 then securely returns the current context awareness information to Context Inference Engine 136 in the wireless device 100.

6. Context Inference Engine 136 in the wireless device 100 then provides the current context awareness information through Context Awareness APIs 154 to the application programs registered for to receive that information.

Figure 2A shows how Web Services in Web Service Server 160 are enabled to receive current context results of the wireless device 100. Web Services Server 160 has a software system for server application program A and an execution environment for server application programs X and Y that are similar to the software system SS1 and execution environment (Exec. Env.) in the wireless device 100 shown in Figure 2. Server Application programs A, X, and Y in Web Service Server 160 may require access through the Context Awareness APIs to provide Web Services with the current context of the wireless device 100.

In Figure 2A, Web Service Server 160 uses the Context Inference Client 176 to contact the Context Inference Server 174 in the network server 140. Context Inference Client 176 may utilize customer database information in database 184 to enhance the context sensitivity capabilities of the web server 160. The contact to the network server

140 is done through a context awareness interface 186 to the Context Inference Server 174 in the network server 140.

Context Inference Server 174 registers the Web Services of the web server 160 through the privacy control 164 of the network server 140 to the Context Inference Engine 142. Privacy control 164 has a cached copy 144 of the Privacy Profile 152 of the wireless device 100. This enables processing of the privacy check in the network Server 140 for access requests from web server 160. The communication between web server 160 and network server 140 is secured using the Internet secure protocols such as HTTPS or SSL. The Context Inference Server 174 can publish its own service as a Web Service to other Web Services on the Internet, in which case the implementation of the interface 186 between web server 160 and network server 140 can be Extensible Markup Language (XML) messages carried in the Simple Object Access Protocol (SOAP) messaging protocol.

The Context inference Engine 142 in the network server 140 will receive processed sensor metadata vector 138 information and possibly some application API information originated from the Context Inference Engine 136 of the wireless device 100. The Context inference Engine 142 of the network server has user database 146 information of the behavior of the user and of the past usage of the wireless device. The Context inference Engine 142 of the network server may also have third party services available (such as instances offering content and/or services) to be offered to potential users. What is offered to the user can also depend on the user profile 144. The nature of the Context inference Engine 136 information of the wireless device 100 that is conveyed to the Context inference Engine 142 of the network can be controlled with the privacy control 150 that is managed by the user of the wireless device 100. The user may thus fully or partly disable the Context inference Engine 142 of the network to control the amount of his/her information that can be used by third party services. The privacy control 150 enables the user to control access by anyone to his/her private information.

The Context inference Engine 136 of the wireless device receives an input from the API interface 154 from the applications A, B, X, or Y located in the wireless device 100. An example would be from a calendar application program indicating that a meeting is starting in 25 minutes time. As another example the calendar application program

indicates that Lisa is having a birthday tomorrow into which you are participating. The Context inference Engine 136 of the wireless device can convey processed result information to the Context inference Engine 142 of the network server. Now in addition to the sensor information, information from the application programs A, B, X, or Y can also be used in the decision making of the Context inference Engine 136 of the wireless device. A combination of the sensor information and information coming from the application programs A, B, X, or Y can be processed by the Context inference Engine 136. The user's behavior or usage patterns can be detected from the sensor and recorded in a the user database, concerning the usage of the application programs. As previously discussed, the processing of this combined information from the sensors and from the application programs can be shared between the Context inference Engine 136 and the Context inference Engine 142. Either the application programs A, B, X, or Y running in the wireless device 100 or the server application programs A, X and Y running in the web server 160, may optionally provide application data to the context inference engine 142 in the network server 140. The context inference engine 142 can optionally process the metadata vector 138 and the application data to produce the current context.

The information transfer from the Context inference Engine 136 of the wireless device to the Context inference Engine 142 of the network server can be done in alternative ways. The system can be managed so that the current consumption and transfer capacity between the wireless device 100 and the network server 140 is taken into account. The context information does not always have to be collected so frequently that it would have to be periodically transferred to the network side 140 every few seconds. Depending on the application, the timing window applied to information transfer from the Context inference Engine 136 of the wireless device 100 to the Context inference Engine 142 of the server 140 can vary from seconds to minutes. If there were no event change or condition change in the environment of the wireless device 100, there would be no need to transfer information to the Context inference Engine 142 of the server 140. Additionally information can be temporarily stored in a buffer in the wireless device 100, which can then transferred less frequently to the network Context inference Engine 142. Packet based GPRS and UMTS can support the less frequent information transfer rates. Also, it is advantageous to send the network Context inference Engine 142 information

from the wireless device 100 as an attachment, immediately subsequent to other signaling made to in the network direction from the wireless device 100, thus saving the radio transmitter of the wireless device 100 from having to be switched on again for transferring the Context inference Engine 136 information separately to the network server 140.

Returning to Figure 1, the relationship is shown between the network server 140, the Universal Description, Discovery and Integration (UDDI) registry 170, and a plurality of web site servers 160. UDDI is a defacto standard for an Internet-based registry. The UDDI registry 170 enables the network server 140 to discover new web sites for services and businesses on the Internet. Once such services and businesses are identified by the UDDI registry 170 to the network server 140, then the server 140 must apply the mobile user's cached privacy profile 144 in Figure 2A, in order to prevent unauthorized access of the user's private data by application programs on the newly discovered web sites.

Figure 3 is a network process flow diagram of the interaction of the wireless device 100 I the first column, network server 140 in the middle column, and web server 160 in the right column, when they carry out the determination of the current context of the wireless device 100. The process begins with the wireless device 100 in step 302:

Step 302: PRIVACY CONTROL 150 IN WIRELESS DEVICE 100 SENDS UPDATED PRIVACY PROFILE TO NETWORK SERVER 140.

Then the network server 140 continues with step 304:

Step 304: NETWORK SERVER 140 UPDATES CACHED PRIVACY PROFILE 144.

The wireless device 100 continues with the following steps 306, 308, and 310:

Step 306: SENSORS CONTINUOUSLY PROVIDE SENSOR DATA TO CONTEXT INFERENCE ENGINE 136 IN WIRELESS DEVICE 100.

Step 308: APPLICATION PROGRAM THAT USES CONTEXT AWARENESS API 154 REQUESTS LATEST CONTEXT INFORMATION.

Step 310: CONTEXT INFERENCE ENGINE 136 CONTACTS CONTEXT INFERENCE ENGINE 142 OF THE NETWORK SERVER 140 AND SENDS THE METADATA VECTOR 138 TO SERVER 140.

Then the network server 140 continues with steps 312 and 314:

Step 312: CONTEXT INFERENCE ENGINE 142 AT NETWORK SERVER 140 USES LOCAL USER INFORMATION STORED IN USER DATABASE 146 TO MAKE A MORE ACCURATE DETERMINATION OF THE MOBILE USER'S CURRENT CONTEXT.

Step 314: NETWORK SERVER 140 REQUESTS DATA FROM WEB SERVER 160.
THE NETWORK SERVER'S ACCESS IS AUTHORIZED BY CACHED PRIVACY PROFILE 144 IN NETWORK SERVER.

Then the web server 160 continues with step 316:

Step 316: WEB SERVER PROVIDES USER INFORMATION STORED IN DATABASE 184 TO NETWORK SERVER 140.

Then the network server 140 continues with step 318:

Step 318: CONTEXT INFERENCE ENGINE 142 AT THE NETWORK SERVER 140 THEN SECURELY RETURNS THE CURRENT CONTEXT AWARENESS INFORMATION TO CONTEXT INFERENCE ENGINE 136 IN THE WIRELESS DEVICE 100.

Then the wireless device 100 finishes with step 320:

Step 318: CONTEXT INFERENCE ENGINE 136 IN THE WIRELESS DEVICE 100 THEN PROVIDES THE CURRENT CONTEXT AWARENESS INFORMATION THROUGH CONTEXT AWARENESS APIs 154 TO THE APPLICATION PROGRAMS REGISTERED TO RECEIVE THAT INFORMATION.

Figure 4 is a functional block diagram of the network server 140, showing the memory 402 storing the application services software programs needed to perform the operations of the invention. The memory is connected by the bus 404 to the cache 144, user database 146, TCP/IP network adapter 406, and central processor 410. The memory 402 stores programs which are sequences of executable instructions which, when executed by the processor 410, carry out the methods of the invention.

Figure 4 is a functional block diagram of the network server, showing the memory storing the application services software programs needed to perform the operations of an embodiment of the invention. Figure 4 discloses the functional components of an exemplary network server 140 arranged as an object model. The object model groups the

object oriented software programs into components that perform the major functions and applications in network server 140. The object model for memory 402 of network server 140 employs a three-tier architecture that includes presentation tier 415, infrastructure objects partition 422, and business logic tier 414. The object model further divides business logic tier 414 into two partitions, application objects partition 422 and data objects partition 426.

Presentation tier 415 retains the programs that manage the device interfaces to network server 140. In Figure 4, presentation tier 415 includes network interface 420. A suitable implementation of presentation tier 415 may use Java servlets to interact with WAP protocol gateway 120 via the hypertext transfer protocol ("HTTP"). The Java servlets ran within a request/response server that manages the exchange of messages between WAP protocol gateway 120 and network server 140. A Java servlet is a Java program that runs within a Web server environment. A Java servlet takes a request as input, parses the data, performs logic operations, and issues a response back to WAP protocol gateway 120. The Java runtime platform pools the Java servlets to simultaneously service many requests. Network interface 420 accepts request messages from WAP protocol gateway 120 and passes the information in the request to visit object 428 for further processing. Visit object 428 passes the result of that processing to network interface 420 for transmission back to the WAP protocol gateway 120. Network interface 420 may also use network adapter 406 to exchange data with another user device.

Infrastructure objects partition 422 retains the programs that perform administrative and system functions on behalf of business logic tier 414. Infrastructure objects partition 422 includes operating system 425, and an object oriented software program component for database server interface 430, and system administrator interface 432.

Business logic tier 414 in Figure 4 includes multiple instances of visit object 428, 428', 428". A separate instance of visit object 428 exists for each network interface 420 session. Each visit object 428 is a stateful session object that includes a persistent storage area from initiation through termination of the session, not just during a single interaction or method call. The persistent storage area retains information associated with the session.

When WAP protocol gateway 120 sends a metadata vector 138 message to network server 140, the message is sent to network interface 420 to invoke a method that creates visit object 428 and stores connection information as a state in visit object 428. Visit object 428 may, in turn, invoke a method in context inference engine 142 application 440 to perform a context inference on the metadata vector and return a current context result.

When WAP protocol gateway 120 sends a privacy control data 150' message to network server 140, the message is sent to network interface 420 to invoke a method that creates visit object 428 and stores connection information as a state in visit object 428. Visit object 428 may, in turn, invoke a method in privacy control 164 application 442 to update the cached privacy profile 144. The application 442, in turn make a method call to privacy profile update application 448 to store the updated data 150' in the cache 144.

When WAP protocol gateway 120 sends a user data update message to network server 140, the message is sent to network interface 420 to invoke a method that creates visit object 428 and stores connection information as a state in visit object 428. Visit object 428 may, in turn, invoke a method in user database application 446 to store the user data in the database 146.

A description of server programming applications developed with Enterprise Java Beans is provided in the book by Ed Roman entitled "Mastering Enterprise Java Beans", published by John Wiley and Sons, 1999. A description of the use of an object model in the design of server applications is provided in the book by Matthew Reynolds entitled "Beginning E-Commerce", Wrox Press Inc, 2000, (ISBN: 1861003986). Java servlets and the development of web site servers is described in the book by Duane K. Fields, et al. entitled "Web Development with Java Server Pages", published by Manning Publications Co., 2000.

The resulting context sensitive web services invention enables a mobile phone or wireless device 100 to use context inference techniques to sense the user's environment and in response, to provide useful information to the user that is appropriate to the user's

perceived environment. The mobile user is provided with the ability to control access by application programs anywhere in the network, to the user's private data.

Although a specific embodiment of the invention has been disclosed, it will be understood by those having skill in the art that changes can be made to the specific embodiment without departing from the spirit and the scope of the invention.

CLAIMS

What is claimed is:

1. A method to enable a wireless device to provide useful information to its user that is appropriate to the device's current environment, comprising:

receiving sensor signals characterizing a current environment of the wireless device;

processing the sensor signals with a context inference engine;

outputting a current context result from the processing by context inference engine; and

providing useful information to the user in response to the current context result.

2. The method of claim 1, wherein the processing of the sensor signals with a context inference engine is embodied as programmed instructions executed within the user's wireless device.

3. The method of claim 1, wherein the processing of the sensor signals with a context inference engine is embodied as programmed instructions executed within a separate network server in response to signals from the user's wireless device.

4. The method of claim 3, wherein the server accesses files from a web server, for selective forwarding to the user's wireless device.

5. The method of claim 3, wherein the wireless device offloads a portion of the processing of the sensor signals with a context inference engine to the server.

6. The method of claim 3, wherein a personal profile of the user is maintained by the server.

7. The method of claim 1, which further comprises:

providing user control of access by application programs to the user's private data.

8. The method of claim 3, which further comprises:

providing user control of access by application programs to the user's private data in the server.

9. The method of claim 1, which further comprises:

providing user control of access by application programs in a web server, to the user's private data.

10. The method of claim 1, which further comprises:

providing the current context result to an application program; and

receiving the useful information for the user from the application program.

11. The method of claim 1, which further comprises:

providing user control of access by an application program to the current context result;

providing the current context result to the application program in response to the user control; and

receiving the useful information from the application program.

12. The method of claim 11, which further comprises:

granting access permission to the application program to access the current context result, based on the user's data stored in a privacy profile.

13. The method of claim 11, wherein providing user control of access is embodied as programmed instructions executed within a separate network server in response to signals from the user's wireless device.

14. The method of claim 13, wherein the server accesses files from a web server, for selective forwarding to the user's wireless device.

15. The method of claim 13, wherein the wireless device offloads a portion of the processing of providing user control of access, to the server.

16. The method of claim 13, wherein a personal profile of the user is maintained by the server.

17. The method of claim 16, which further comprises:

providing user control of access by application programs to the user's personal profile.

18. The method of claim 13, which further comprises:

providing user control of access by application programs to the user's personal profile in the server.

19. The method of claim 11, which further comprises:

providing user control of access by application programs in a web server, to the user's private data.

20. The method of claim 19, which further comprises:

enabling context sensitive applications and services within the wireless device while providing to the user control over the privacy user's current context result.

21. The method of claim 19, which further comprises:

enabling context sensitive applications and services within the network server while providing to the user control over the privacy user's current context result.

22. An apparatus to enable a wireless device to provide useful information to its user that is appropriate to the device's current environment, comprising:

a processor;

a memory coupled to the processor, programmed to perform the steps of:

receiving sensor signals characterizing a current environment of the wireless device;

processing the sensor signals with a context inference engine;

outputting a current context result from the processing by context inference engine; and

providing useful information to the user in response to the current context result.

23. The apparatus of claim 22, wherein the processing of the sensor signals with a context inference engine is embodied as programmed instructions executed within the user's wireless device.

24. The apparatus of claim 22, wherein the processing of the sensor signals with a context inference engine is embodied as programmed instructions executed within a separate network server in response to signals from the user's wireless device.

25. The apparatus of claim 24, wherein the server accesses files from a web server, for selective forwarding to the user's wireless device.

26. A wireless device to provide useful information to its user that is appropriate to the device's current environment, comprising:

a sensor for providing sensor signals characterizing a current environment of the wireless device;

a context inference engine coupled to the sensor, for processing the sensor signals;

said context inference engine providing a current context result from the processing; and

an output device coupled to the context inference engine, for providing useful information to the user in response to the current context result.

27. A wireless device to provide useful information to its user that is appropriate to the device's current environment, comprising:

a privacy control for providing the user control of access by an application program to the user's private data;

a sensor for providing sensor signals characterizing a current environment of the wireless device;

a context inference engine coupled to the sensor, for processing the sensor signals;

said context inference engine coupled to the privacy control, for providing a current context result from the processing to the application program; and

an output device coupled to the privacy control, for providing useful information to the user in response to the application program.

28. A system to provide useful information to the user of a wireless device that is appropriate to the device's current environment, comprising:

a privacy control in a server for receiving a user privacy profile from the wireless device and providing the user control of access by an application program to the user's private data;

a sensor in the wireless device for providing sensor signals characterizing a current environment of the wireless device;

a context inference engine in the server coupled to the wireless device, for processing sensor information derived from the sensor signals;

said context inference engine coupled to the privacy control, for providing a current context result from the processing to the application program; and

an output device in the server, coupled to the privacy control, for transmitting useful information to the wireless device in response to the application program.

29. A method to enable a wireless device to provide useful information to its user that is appropriate to the device's current environment, comprising:

running a program that provides application data to the wireless device;

receiving sensor signals characterizing a current environment of the wireless device;

processing the sensor signals and the application data with a context inference engine;

outputting a current context result from the processing by context inference engine; and

providing useful information to the user in response to the current context result.

30. The method of claim 29, wherein the processing of the sensor signals with a context inference engine is embodied as programmed instructions executed within the user's wireless device.

31. The method of claim 30, wherein the step of running a program occurs in the wireless device.

32. The method of claim 29, wherein the processing of the sensor signals with a context inference engine is embodied as programmed instructions executed within a separate network server in response to signals from the user's wireless device.

33. The method of claim 32, wherein the step of running a program occurs in a web server coupled to the network server.

34. A system to enable a wireless device to provide useful information to its user that is appropriate to the device's current environment, comprising:

a processor;

a memory coupled to the processor, programmed to perform the steps of:

running a program that provides application data to the wireless device;

receiving sensor signals characterizing a current environment of the wireless device;

processing the sensor signals and the application data with a context inference engine;

outputting a current context result from the processing by context inference engine; and

providing useful information to the user in response to the current context result.

35. The system of claim 34, wherein the processing of the sensor signals and the application data with a context inference engine is embodied as programmed instructions executed within the user's wireless device.

36. The system of claim 35, wherein the step of running a program occurs in the wireless device.

37. The system of claim 34, wherein the processing of the sensor signals and the application data with a context inference engine is embodied as programmed instructions executed within a separate network server in response to signals from the user's wireless device.

38. The system of claim 37, wherein the step of running a program occurs in a web server coupled to the network server.

39. A method to enable a wireless device to provide useful information to its user that is appropriate to the device's current environment, comprising:

receiving sensor signals characterizing a current environment of the wireless device;

partially processing the sensor signals with a first context inference engine within the user's wireless device;

sending the partially processed sensor signals to a second context inference engine within a separate network server;

completing the processing the sensor signals with the second context inference engine;

sending a current context result from the second context inference engine to the wireless device; and

providing useful information to the user in response to the current context result.

40. A system to enable a wireless device to provide useful information to its user that is appropriate to the device's current environment, comprising:

a wireless device for receiving sensor signals characterizing a current environment of the wireless device;

a first context inference engine within the user's wireless device for partially processing the sensor signals;

a second context inference engine within a separate network server for receiving the partially processed sensor signals sent from the wireless device and completing the processing the sensor signals;

said second context inference engine sending a current context result from the second context inference engine to the wireless device; and

said wireless device providing useful information to the user in response to the current context result.

41. A method to enable a wireless device to provide useful information to its user that is appropriate to the device's current environment, comprising:

receiving sensor signals characterizing a current environment of the wireless device;

partially processing the sensor signals with a first context inference engine within the user's wireless device;

sending the partially processed sensor signals to a second context inference engine within a separate network server;

completing the processing the sensor signals with the second context inference engine;

forwarding a current context result from the network server to a second server; and

sending useful information from the second server to the user's wireless device in response to the current context result.

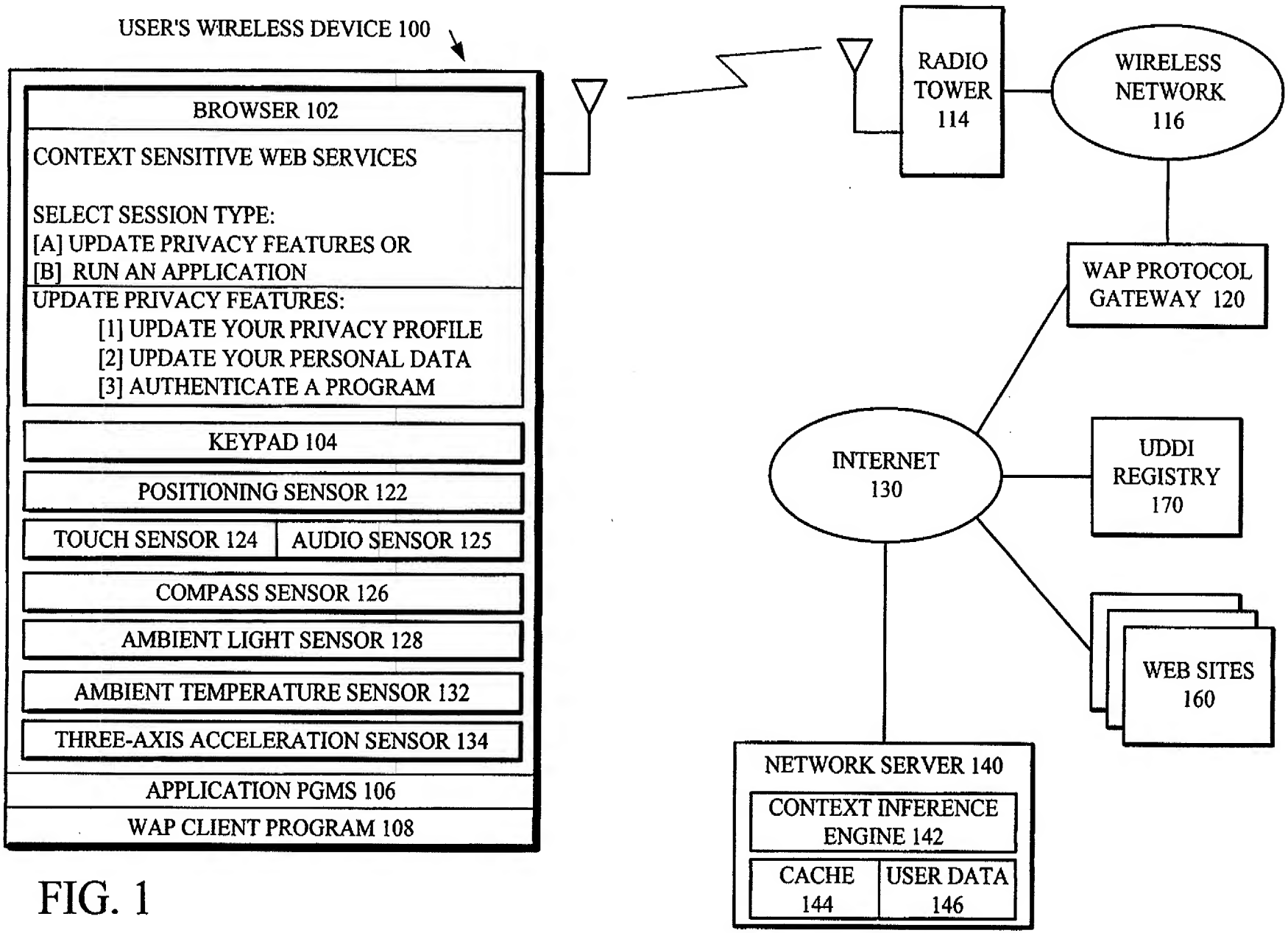

USER'S WIRELESS DEVICE 100
BROWSER 102
CONTEXT SENSITIVE WEB SERVICES
SELECT SESSION TYPE:
[A] UPDATE PRIVACY FEATURES OR
[B] RUN AN APPLICATION
UPDATE PRIVACY FEATURES:
[1] UPDATE YOUR PRIVACY PROFILE
[2] UPDATE YOUR PERSONAL DATA
[3] AUTHENTICATE A PROGRAM
KEYPAD 104
POSITIONING SENSOR 122
TOUCH SENSOR 124
AUDIO SENSOR 125
COMPASS SENSOR 126
AMBIENT LIGHT SENSOR 128
AMBIENT TEMPERATURE SENSOR 132
THREE-AXIS ACCELERATION SENSOR 134
APPLICATION PGMS 106
WAP CLIENT PROGRAM 108
RADIO TOWER 114
WIRELESS NETWORK 116
WAP PROTOCOL GATEWAY 120
INTERNET 130
UDDI REGISTRY 170
WEB SITES 160
NETWORK SERVER 140
CONTEXT INFERENCE ENGINE 142
CACHE 144
USER DATA 146

FIG. 1

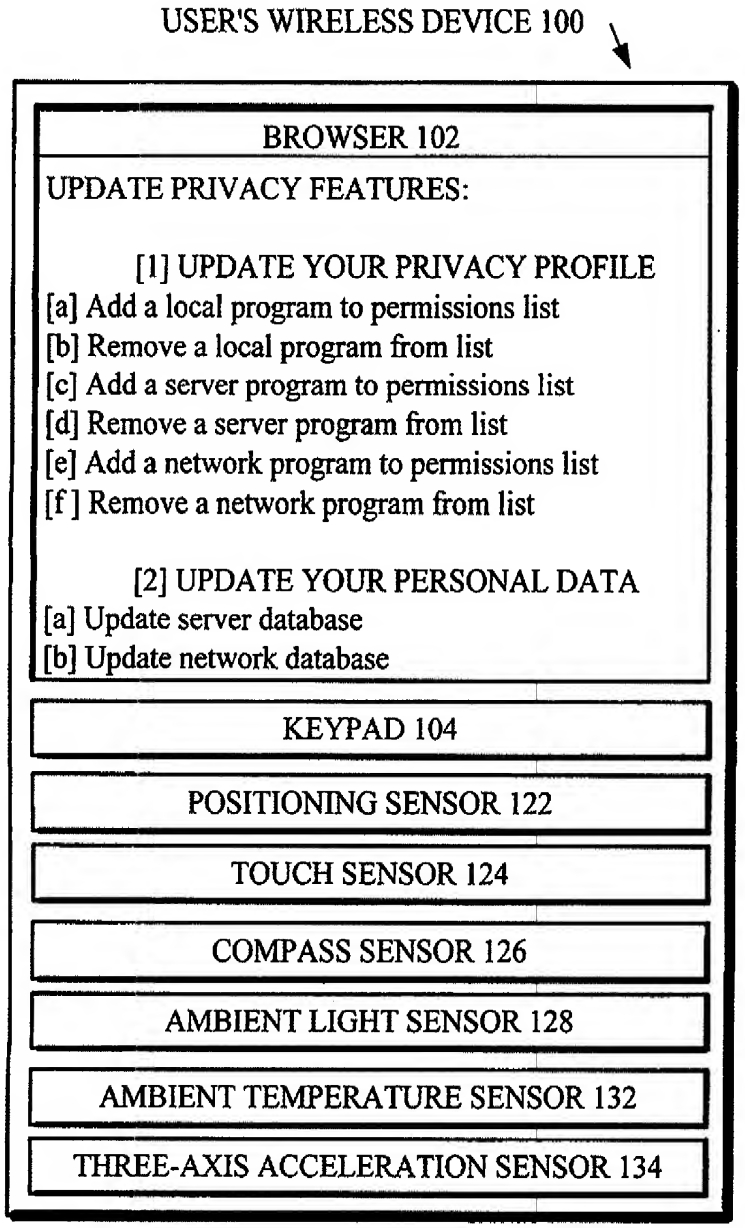

USER'S WIRELESS DEVICE 100
BROWSER 102
UPDATE PRIVACY FEATURES:
[1] UPDATE YOUR PRIVACY PROFILE
[a] Add a local program to permissions list
[b] Remove a local program from list
[c] Add a server program to permissions list
[d] Remove a server program from list
[e] Add a network program to permissions list
[f] Remove a network program from list
[2] UPDATE YOUR PERSONAL DATA
[a] Update server database
[b] Update network database
KEYPAD 104
POSITIONING SENSOR 122
TOUCH SENSOR 124
COMPASS SENSOR 126
AMBIENT LIGHT SENSOR 128
AMBIENT TEMPERATURE SENSOR 132
THREE-AXIS ACCELERATION SENSOR 134

FIG. 1A

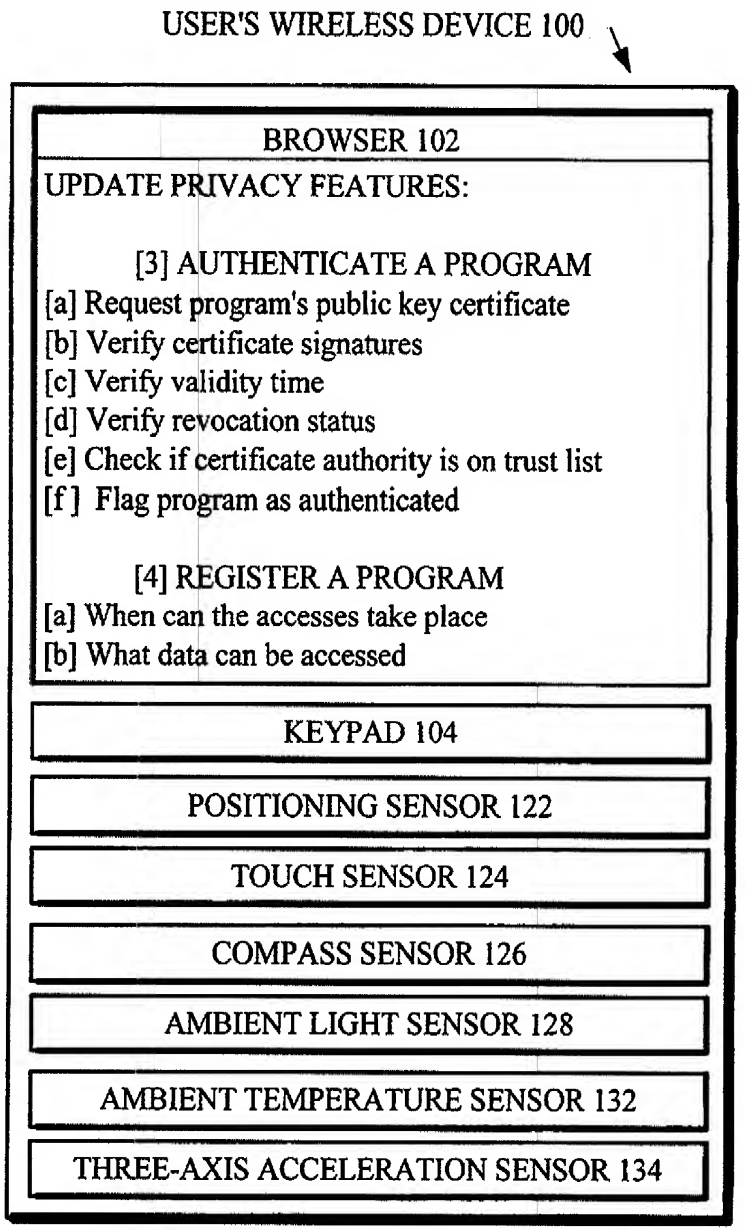

USER'S WIRELESS DEVICE 100
BROWSER 102
UPDATE PRIVACY FEATURES:
[3] AUTHENTICATE A PROGRAM
[a] Request program's public key certificate
[b] Verify certificate signatures
[c] Verify validity time
[d] Verify revocation status
[e] Check if certificate authority is on trust list
[f] Flag program as authenticated
[4] REGISTER A PROGRAM
[a] When can the accesses take place
[b] What data can be accessed
KEYPAD 104
POSITIONING SENSOR 122
TOUCH SENSOR 124
COMPASS SENSOR 126
AMBIENT LIGHT SENSOR 128
AMBIENT TEMPERATURE SENSOR 132
THREE-AXIS ACCELERATION SENSOR 134

FIG. 1B

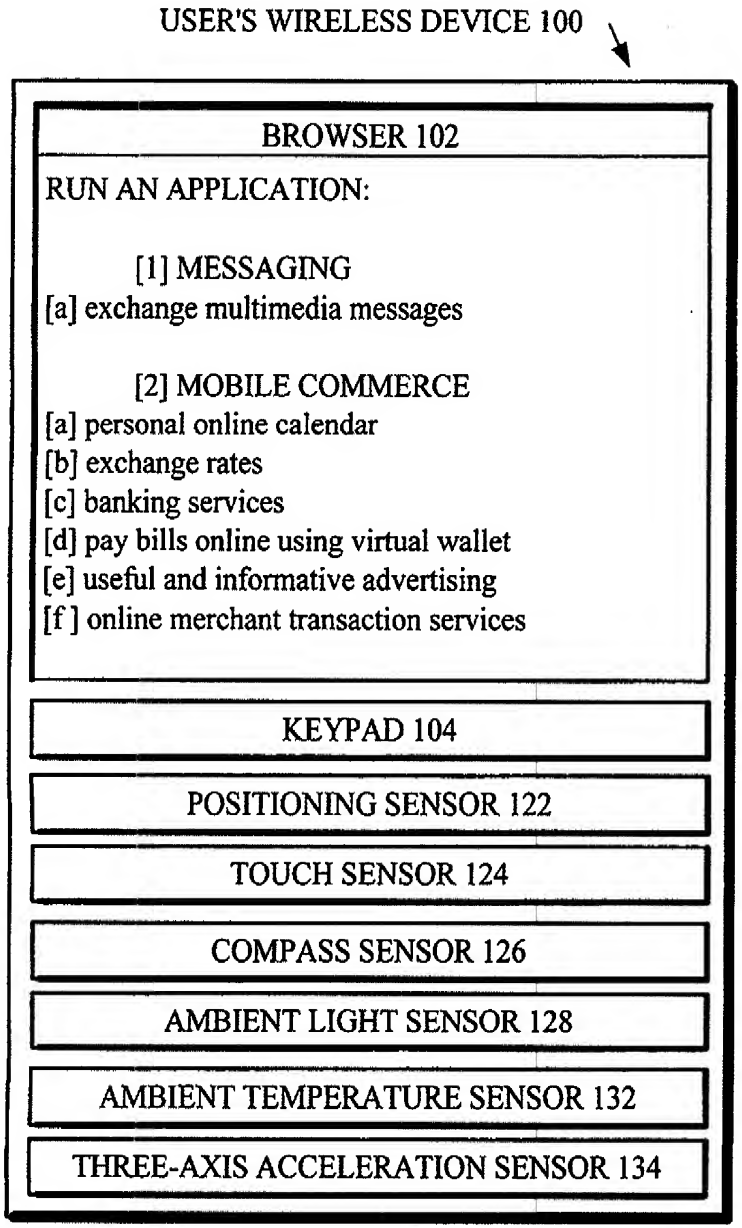

USER'S WIRELESS DEVICE 100
BROWSER 102
RUN AN APPLICATION:
[1] MESSAGING
[a] exchange multimedia messages
[2] MOBILE COMMERCE
[a] personal online calendar
[b] exchange rates
[c] banking services
[d] pay bills online using virtual wallet
[e] useful and informative advertising
[f] online merchant transaction services
KEYPAD 104
POSITIONING SENSOR 122
TOUCH SENSOR 124
COMPASS SENSOR 126
AMBIENT LIGHT SENSOR 128
AMBIENT TEMPERATURE SENSOR 132
THREE-AXIS ACCELERATION SENSOR 134

FIG. 1C

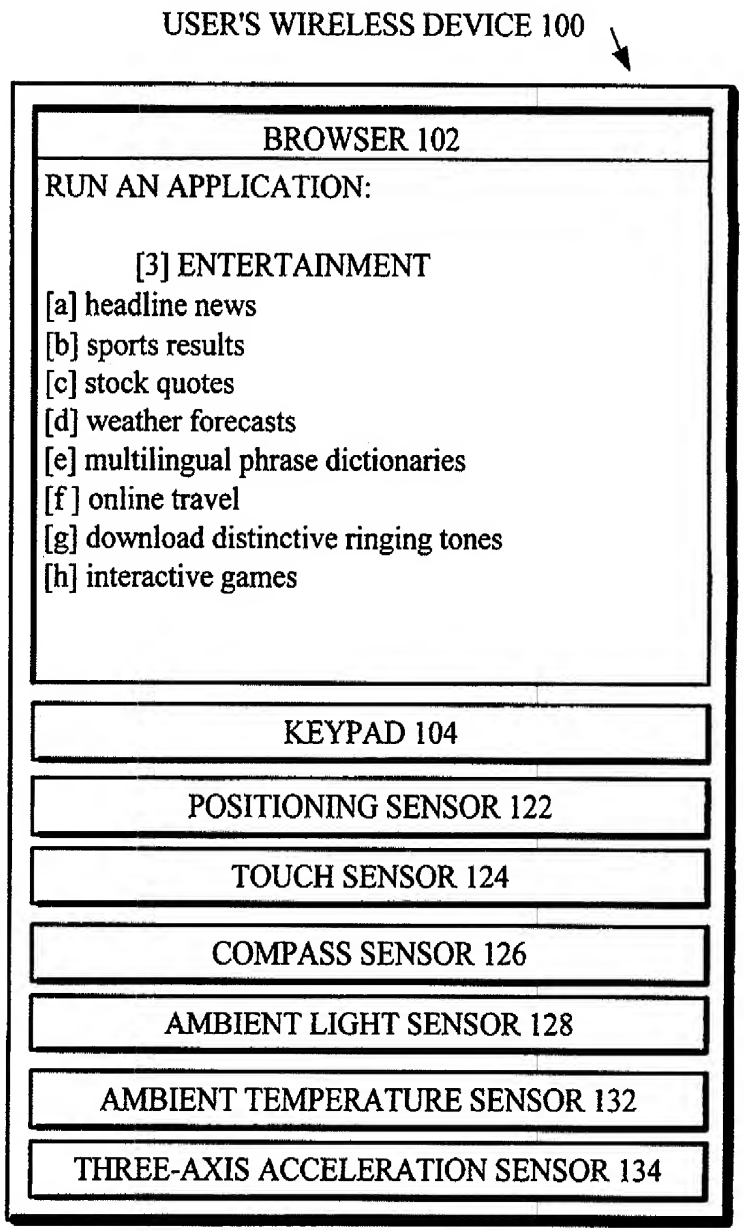

USER'S WIRELESS DEVICE 100
BROWSER 102
RUN AN APPLICATION:
[3] ENTERTAINMENT
[a] headline news
[b] sports results
[c] stock quotes
[d] weather forecasts
[e] multilingual phrase dictionaries
[f] online travel
[g] download distinctive ringing tones
[h] interactive games
KEYPAD 104
POSITIONING SENSOR 122
TOUCH SENSOR 124
COMPASS SENSOR 126
AMBIENT LIGHT SENSOR 128
AMBIENT TEMPERATURE SENSOR 132
THREE-AXIS ACCELERATION SENSOR 134

FIG. 1D

FIG. 2

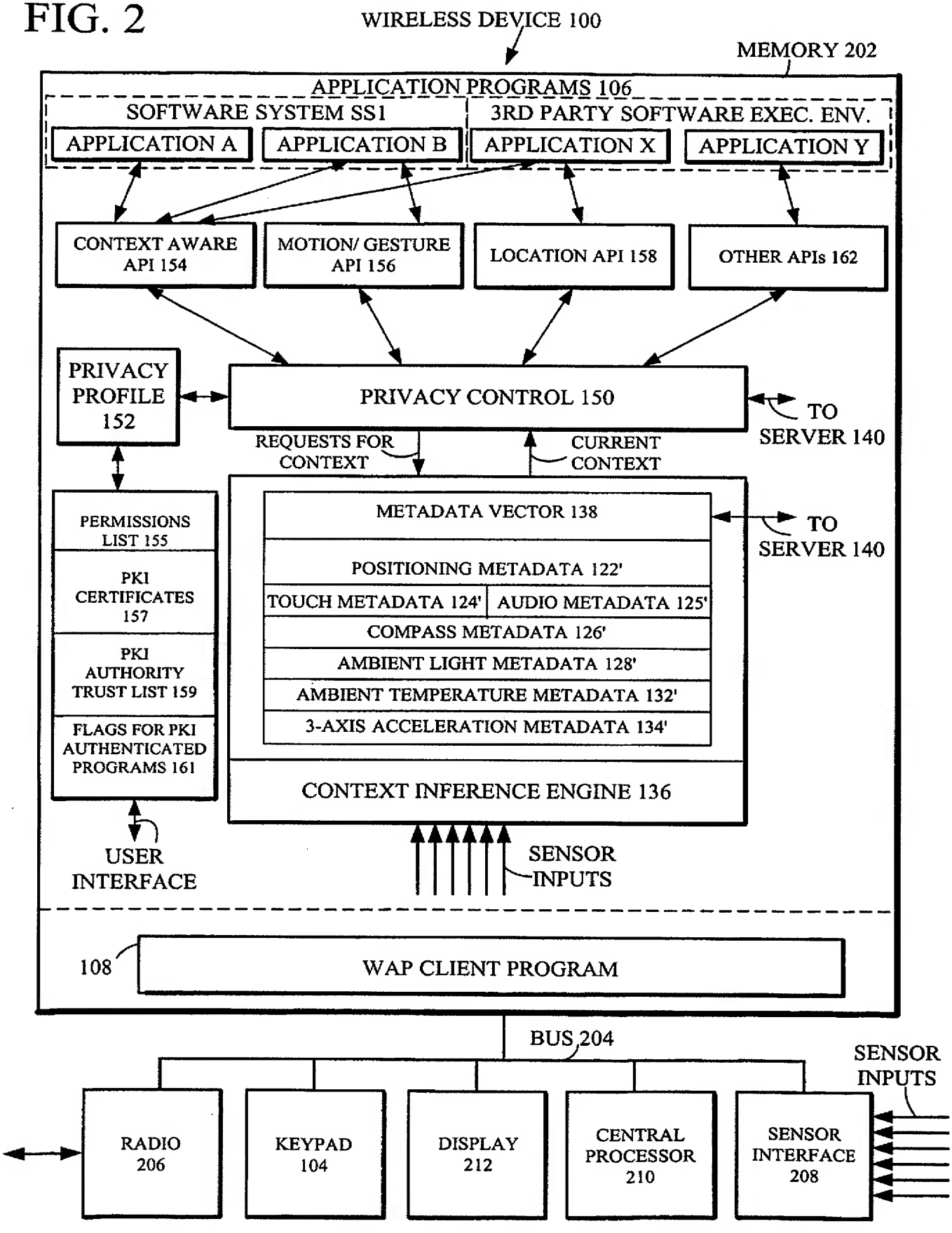

WIRELESS DEVICE 100
MEMORY 202
APPLICATION PROGRAMS 106
SOFTWARE SYSTEM SS1
3RD PARTY SOFTWARE EXEC. ENV.
APPLICATION A
APPLICATION B
APPLICATION X
APPLICATION Y
CONTEXT AWARE API 154
MOTION/ GESTURE API 156
LOCATION API 158
OTHER APIs 162
PRIVACY PROFILE 152
PRIVACY CONTROL 150
TO SERVER 140
REQUESTS FOR CONTEXT
CURRENT CONTEXT
PERMISSIONS LIST 155
PKI CERTIFICATES 157
PKI AUTHORITY TRUST LIST 159
FLAGS FOR PKI AUTHENTICATED PROGRAMS 161
METADATA VECTOR 138
TO SERVER 140
POSITIONING METADATA 122'
TOUCH METADATA 124'
AUDIO METADATA 125'
COMPASS METADATA 126'
AMBIENT LIGHT METADATA 128'
AMBIENT TEMPERATURE METADATA 132'
3-AXIS ACCELERATION METADATA 134'
CONTEXT INFERENCE ENGINE 136
USER INTERFACE
SENSOR INPUTS
108
WAP CLIENT PROGRAM
BUS 204
SENSOR INPUTS
RADIO 206
KEYPAD 104
DISPLAY 212
CENTRAL PROCESSOR 210
SENSOR INTERFACE 208

FIG. 2A

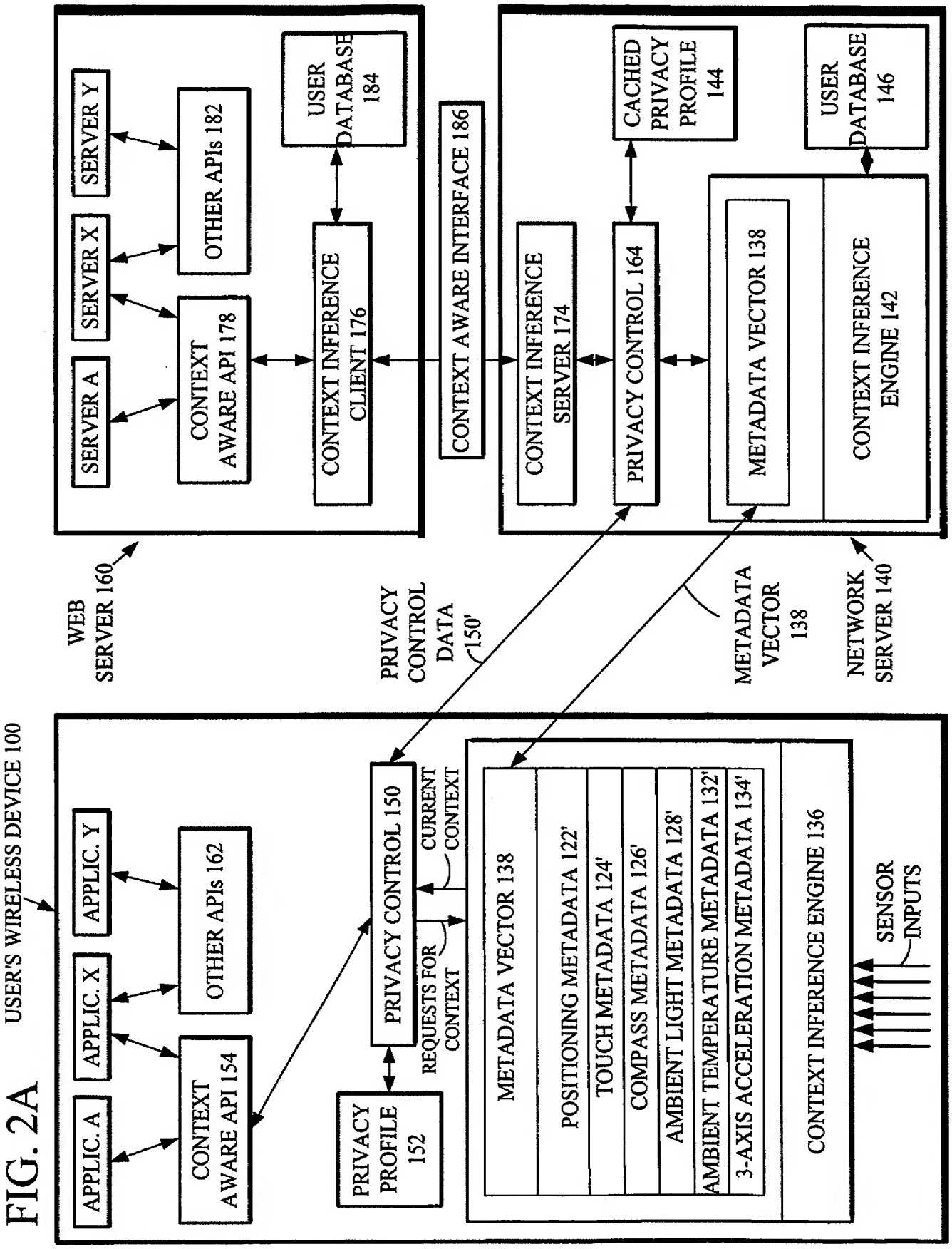

USER'S WIRELESS DEVICE 100
APPLIC. A
APPLIC. X
APPLIC. Y
CONTEXT AWARE API 154
OTHER APIs 162
PRIVACY PROFILE 152
PRIVACY CONTROL 150
REQUESTS FOR CONTEXT
CURRENT CONTEXT
METADATA VECTOR 138
POSITIONING METADATA 122'
TOUCH METADATA 124'
COMPASS METADATA 126'
AMBIENT LIGHT METADATA 128'
AMBIENT TEMPERATURE METADATA 132'
3-AXIS ACCELERATION METADATA 134'
CONTEXT INFERENCE ENGINE 136
SENSOR INPUTS
WEB SERVER 160
SERVER A
SERVER X
SERVER Y
CONTEXT AWARE API 178
OTHER APIs 182
CONTEXT INFERENCE CLIENT 176
USER DATABASE 184
CONTEXT AWARE INTERFACE 186
CONTEXT INFERENCE SERVER 174
PRIVACY CONTROL 164
CACHED PRIVACY PROFILE 144
METADATA VECTOR 138
CONTEXT INFERENCE ENGINE 142
USER DATABASE 146
PRIVACY CONTROL DATA 150'
METADATA VECTOR 138
NETWORK SERVER 140

FIG. 3

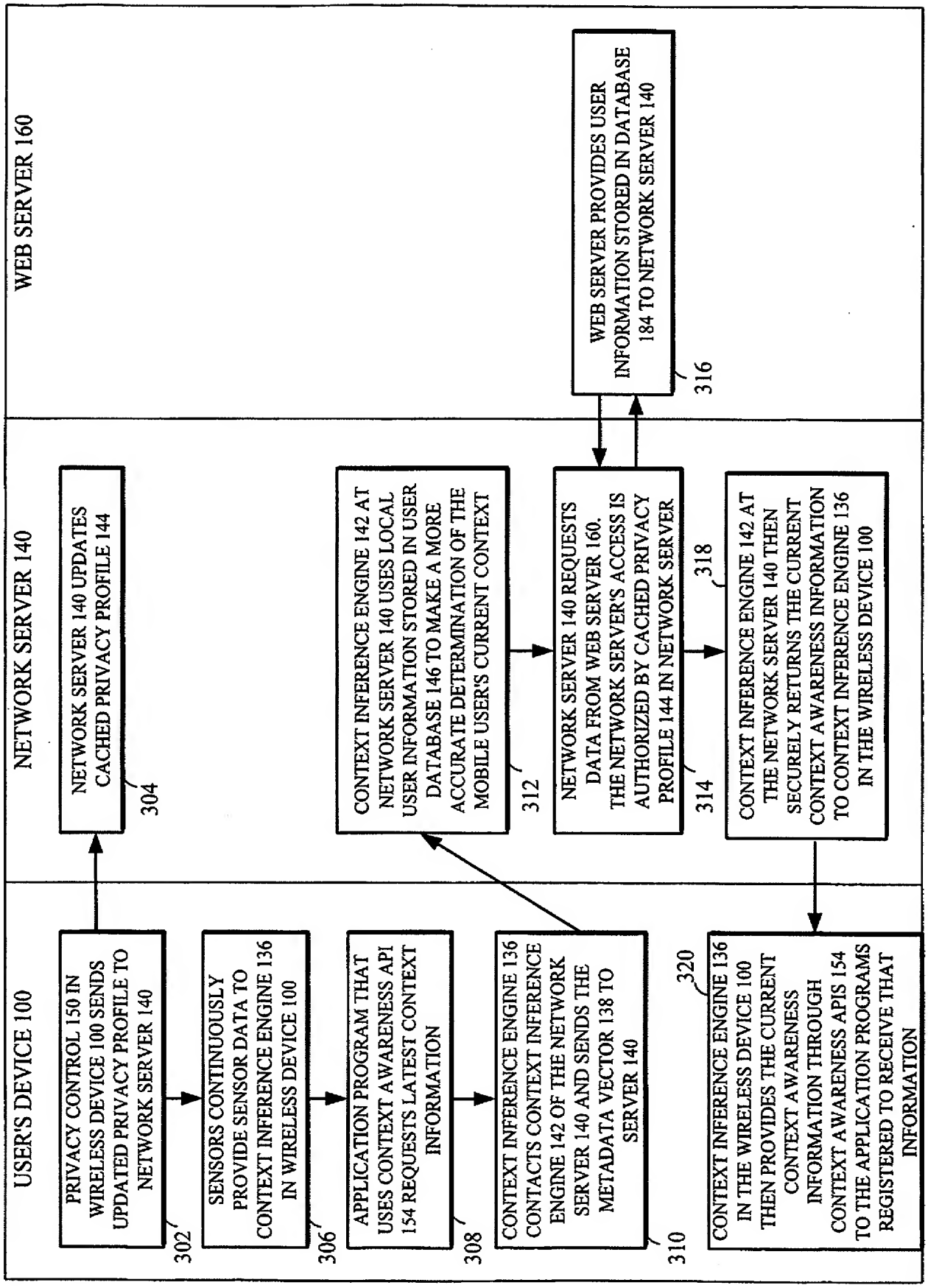
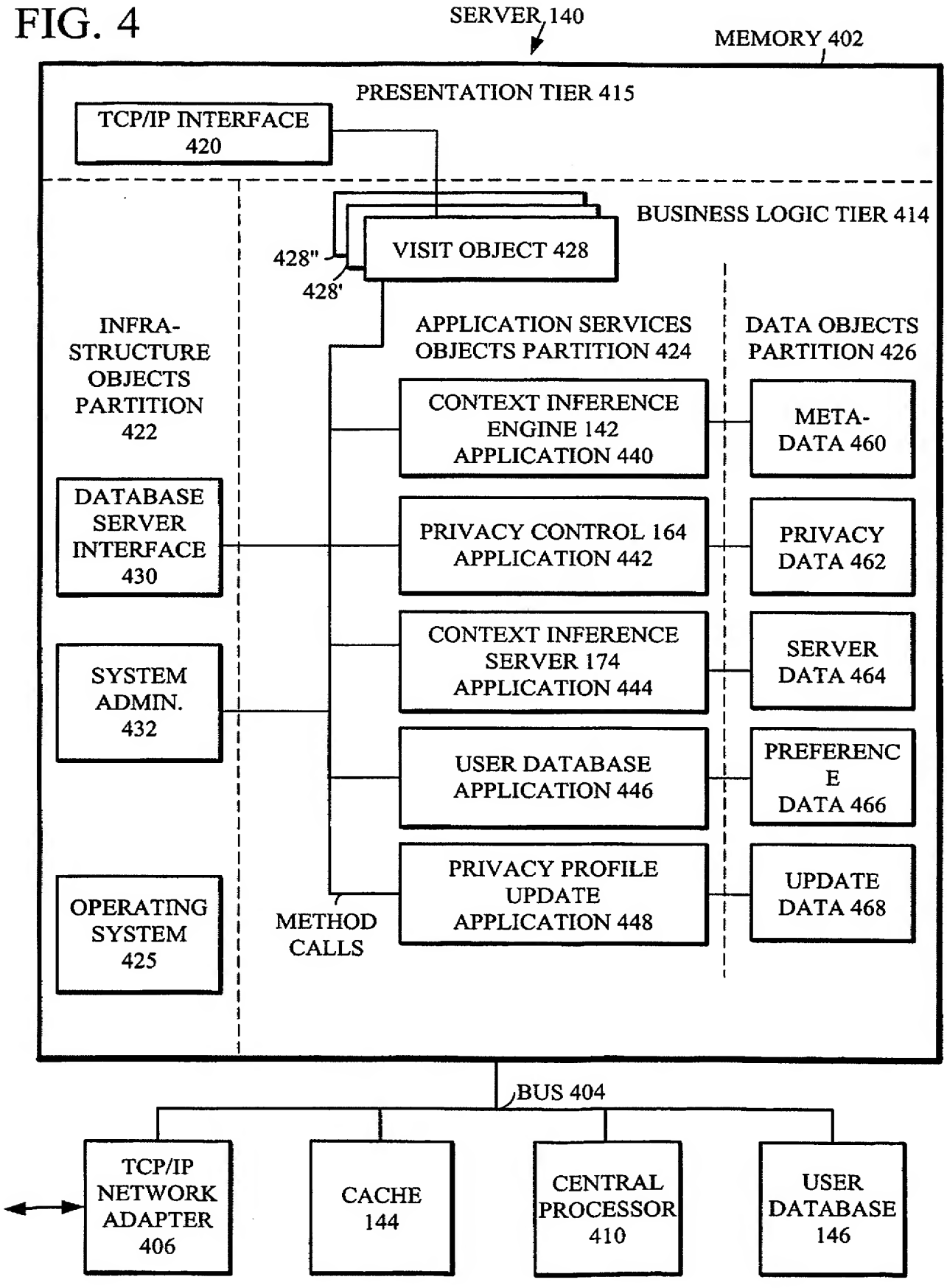

USER'S DEVICE 100
NETWORK SERVER 140
WEB SERVER 160
PRIVACY CONTROL 150 IN WIRELESS DEVICE 100 SENDS UPDATED PRIVACY PROFILE TO NETWORK SERVER 140
302
NETWORK SERVER 140 UPDATES CACHED PRIVACY PROFILE 144
304
SENSORS CONTINUOUSLY PROVIDE SENSOR DATA TO CONTEXT INFERENCE ENGINE 136 IN WIRELESS DEVICE 100
306
APPLICATION PROGRAM THAT USES CONTEXT AWARENESS API 154 REQUESTS LATEST CONTEXT INFORMATION
308
CONTEXT INFERENCE ENGINE 136 CONTACTS CONTEXT INFERENCE ENGINE 142 OF THE NETWORK SERVER 140 AND SENDS THE METADATA VECTOR 138 TO SERVER 140
310
CONTEXT INFERENCE ENGINE 142 AT NETWORK SERVER 140 USES LOCAL USER INFORMATION STORED IN USER DATABASE 146 TO MAKE A MORE ACCURATE DETERMINATION OF THE MOBILE USER'S CURRENT CONTEXT
312
NETWORK SERVER 140 REQUESTS DATA FROM WEB SERVER 160. THE NETWORK SERVER'S ACCESS IS AUTHORIZED BY CACHED PRIVACY PROFILE 144 IN NETWORK SERVER
314
WEB SERVER PROVIDES USER INFORMATION STORED IN DATABASE 184 TO NETWORK SERVER 140
316
CONTEXT INFERENCE ENGINE 142 AT THE NETWORK SERVER 140 THEN SECURELY RETURNS THE CURRENT CONTEXT AWARENESS INFORMATION TO CONTEXT INFERENCE ENGINE 136 IN THE WIRELESS DEVICE 100
318
CONTEXT INFERENCE ENGINE 136 IN THE WIRELESS DEVICE 100 THEN PROVIDES THE CURRENT CONTEXT AWARENESS INFORMATION THROUGH CONTEXT AWARENESS APIS 154 TO THE APPLICATION PROGRAMS REGISTERED TO RECEIVE THAT INFORMATION
320

FIG. 4


SERVER 140
MEMORY 402
PRESENTATION TIER 415
TCP/IP INTERFACE 420
BUSINESS LOGIC TIER 414
VISIT OBJECT 428
428"
428'
INFRA-STRUCTURE OBJECTS PARTITION 422
APPLICATION SERVICES OBJECTS PARTITION 424
DATA OBJECTS PARTITION 426
CONTEXT INFERENCE ENGINE 142 APPLICATION 440
META-DATA 460
DATABASE SERVER INTERFACE 430
PRIVACY CONTROL 164 APPLICATION 442
PRIVACY DATA 462
CONTEXT INFERENCE SERVER 174 APPLICATION 444
SERVER DATA 464
SYSTEM ADMIN. 432
USER DATABASE APPLICATION 446
PREFERENCE DATA 466
PRIVACY PROFILE UPDATE APPLICATION 448
UPDATE DATA 468
OPERATING SYSTEM 425
METHOD CALLS
BUS 404
TCP/IP NETWORK ADAPTER 406
CACHE 144
CENTRAL PROCESSOR 410
USER DATABASE 146

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB02/01550

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04M 1/00, 3/00, 3/42, 11/10; H04B 1/38
US CL : 455/3.03, 402, 405, 412-420, 456, 458, 466, 515, 550, 556, 575

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 455/3.03, 402, 405, 412-420, 456, 458, 466, 515, 550, 556, 575

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
NONE

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,115,611 A (KIMOTO et al) 05 September 2000, figs. 1, 7-8, 10, 12, 19, 27, 31, 42.	1-38
---		---
Y		39-41
Y	US 6,073,075 A (KONDOU et al) 06 June 2000, fig. 3, column 4 lines 26-42.	39-41

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
19 July 2002 (19.07.2002)

Date of mailing of the international search report
27 AUG 2002

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703)305-3230

Authorized officer
William Trost
Telephone No. 703 306-0377

Form PCT/ISA/210 (second sheet) (July 1998)

第 6 部門第 3 区分

全 18 頁

(19)日本国特許庁(JP)

(12)公表特許公報(A)

(11)特許出願公表番号

特表2004-535000

(P2004-535000A)

(43)公表日 平成16年11月18日(2004.11.18)

(51)Int.Cl.[7]	F I			テーマコード（参考）
G06F 15/00	G06F	15/00	310A	5B085
H04M 11/00	H04M	11/00	302	5K067
H04Q 7/20	H04Q	7/04	Z	5K101

審査請求 未請求 予備審査請求 有 （全 75 頁）

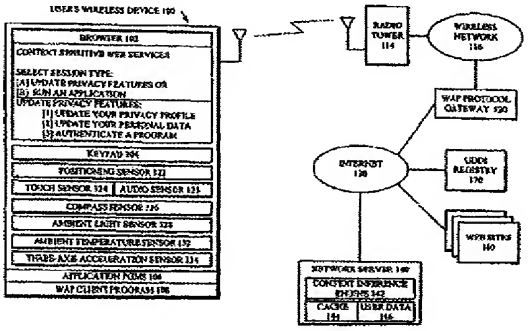
(21)出願番号 特願2002-590624(P2002-590624)
(86)(22)出願日 平成14年5月7日(2002.5.7)
(85)翻訳文提出日 平成15年11月17日(2003.11.17)
(86)国際出願番号 PCT/IB2002/001550
(87)国際公開番号 WO2002/093877
(87)国際公開日 平成14年11月21日(2002.11.21)
(31)優先権主張番号 09/854,628
(32)優先日 平成13年5月15日(2001.5.15)
(33)優先権主張国 米国(US)

(71)出願人 398012616
ノキア コーポレイション
フィンランド エフイーエン－０２１５０
エスプー ケイララーデンティエ 4
(74)代理人 100099759
弁理士 青木 篤
(74)代理人 100092624
弁理士 鶴田 準一
(74)代理人 100102819
弁理士 島田 哲郎
(74)代理人 100122965
弁理士 水谷 好男
(74)代理人 100082898
弁理士 西山 雅也

最終頁に続く

(54)【発明の名称】状況に応じたウェブサービス

(57)【要約】
状況に応じたウェブサービス方法により、携帯電話又は無線装置（１００）は、状況推定技法を使用してユーザーの環境を感知し、これに応答して、感知されたユーザー環境に適した有用な情報をユーザーに提供することができる。この方法は、無線装置（１００）の現在の環境を特徴付けるセンサ信号（１２２～１３４）を受信するステップと、状況推定エンジン（１４２）によってセンサ信号を処理するステップと、状況推定エンジン（１４２）による処理によって生成された現在の状況に関する結果を出力するステップと、この現在の状況に関する結果に応答して有用な情報をユーザーに提供するステップと、を含んでいる。



【特許請求の範囲】
【請求項１】
無線装置が、該装置の現在の環境に適した有用な情報をそのユーザーに提供できるようにする方法であって、
前記無線装置の現在の環境を特徴付けるセンサ信号を受信するステップと、
前記センサ信号を状況推定エンジンによって処理するステップと、
前記状況推定エンジンによる処理によって生成された現在の状況に関する結果を出力するステップと、
前記現在の状況に関する結果に応答し、前記ユーザーに有用な情報を提供するステップと、
を有する方法。
【請求項２】
前記状況推定エンジンによるセンサ信号の処理は、前記ユーザーの無線装置内で稼動するプログラムされた命令として実施される請求項１記載の方法。
【請求項３】
前記状況推定エンジンによるセンサ信号の処理は、前記ユーザーの無線装置からの信号に応答し、別個のネットワークサーバー内で稼動するプログラムされた命令として実行される請求項１記載の方法。
【請求項４】
前記サーバーは、前記ユーザーの無線装置に対して選択的に転送するべく、ウェブサーバーのファイルにアクセスする請求項３記載の方法。
【請求項５】
前記無線装置は、前記状況推定エンジンによるセンサ信号の処理の一部を前記サーバーに負荷分散する請求項３記載の方法。
【請求項６】
前記ユーザーのパーソナルプロファイルを前記サーバーが保持する請求項３記載の方法。
【請求項７】
アプリケーションプログラムによる前記ユーザープライベートデータに対するアクセスのユーザー制御を提供するステップを更に有する請求項１記載の方法。
【請求項８】
アプリケーションプログラムによる前記サーバー内の前記ユーザープライベートデータに対するアクセスのユーザー制御を提供するステップを更に有する請求項３記載の方法。
【請求項９】
ウェブサーバー内のアプリケーションプログラムによる前記ユーザープライベートデータに対するアクセスのユーザー制御を提供するステップを更に有する請求項１記載の方法。
【請求項１０】
前記現在の状況に関する結果をアプリケーションプログラムに提供するステップと、
前記アプリケーションプログラムから前記ユーザーに対する有用な情報を受信するステップと、
を更に有する請求項１記載の方法。
【請求項１１】
アプリケーションプログラムによる前記現在の状況に関する結果に対するアクセスのユーザー制御を提供するステップと、
前記ユーザー制御に応答し、前記現在の状況に関する結果を前記アプリケーションプログラムに提供するステップと、
前記アプリケーションプログラムから前記有用な情報を受信するステップと、
を更に有する請求項１記載の方法。
【請求項１２】
プライバシープロファイル内に保存された前記ユーザーのデータに基づいて、前記現在の状況に関する結果にアクセスするためのアクセス許可を前記アプリケーションプログラムに対して付与するステップを更に有する請求項１１記載の方法。
【請求項１３】
前記アクセスのユーザー制御を提供するステップが、前記ユーザーの無線装置からの信号に応答し、別個のネットワークサーバー内で稼動するプログラムされた命令として実施される請求項１１記載の方法。
【請求項１４】
前記サーバーは、前記ユーザーの無線装置に対して選択的に転送するべく、ウェブサーバーのファイルにアクセスする請求項１３記載の方法。
【請求項１５】
前記無線装置は、前記アクセスのユーザー制御を提供するステップの処理の一部を前記サーバーに負荷分散する請求項１３記載の方法。
【請求項１６】
前記ユーザーのパーソナルプロファイルを前記サーバーが保持する請求項１３記載の方法。
【請求項１７】
アプリケーションプログラムによる前記ユーザーパーソナルプロファイルに対するアクセスのユーザー制御を提供するステップを更に有する請求項１６記載の方法。
【請求項１８】
アプリケーションプログラムによる前記サーバー内の前記ユーザーパーソナルプロファイルに対するアクセスのユーザー制御を提供するステップを更に有する請求項１３記載の方法。
【請求項１９】
ウェブサーバー内のアプリケーションプログラムによる前記ユーザープライベートデータに対するアクセスのユーザー制御を提供するステップを更に有する請求項１１記載の方法。
【請求項２０】
前記プライベートなユーザーの現在の状況に関する結果に対するユーザー制御を提供しつつ、前記無線装置内の状況に応じたアプリケーション及びサービスを実現するステップを更に有する請求項１９記載の方法。
【請求項２１】
前記プライベートなユーザーの現在の状況に関する結果に対するユーザー制御を提供しつつ、前記ネットワークサーバー内の状況に応じたアプリケーション及びサービスを実現するステップを更に有する請求項１９記載の方法。
【請求項２２】
無線装置が、該装置の現在の環境に適した有用な情報をそのユーザーに対して提供できるようにする装置であって、
プロセッサと；
前記プロセッサに接続されたメモリであって、
前記無線装置の現在の環境を特徴付けるセンサ信号を受信するステップと、
前記センサ信号を状況推定エンジンによって処理するステップと、
前記状況推定エンジンによる処理によって生成された現在の状況に関する結果を出力するステップと、
前記現在の状況に関する結果に応答し、前記ユーザーに対して有用な情報を提供するステップと、
を実行するべくプログラムされたメモリと；
を有する装置。
【請求項２３】
前記状況推定エンジンによるセンサ信号の処理は、前記ユーザーの無線装置内で稼動するプログラムされた命令として実施される請求項２２記載の装置。
【請求項２４】
前記状況推定エンジンによるセンサ信号の処理は、前記ユーザーの無線装置からの信号に応答し、別個のネットワークサーバー内で稼動するプログラムされた命令として実施される請求項２２記載の装置。
【請求項２５】
前記サーバーは、前記ユーザーの無線装置に対して選択的に転送するべく、ウェブサーバーのファイルにアクセスする請求項２４記載の装置。
【請求項２６】
無線装置の現在の環境に適した有用な情報をそのユーザーに提供する前記無線装置であって、
前記無線装置の現在の環境を特徴付けるセンサ信号を供給するセンサと、

前記センサに接続され、前記センサ信号を処理し、前記処理によって生成された現在の状況に関する結果を提供する状況推定エンジンと、
前記状況推定エンジンに接続され、前記現在の状況に関する結果に応答し、有用な情報を前記ユーザーに提供する出力装置と、
を有する無線装置。
【請求項２７】
無線装置の現在の環境に適した有用な情報をそのユーザーに提供する前記無線装置であって、
アプリケーションプログラムによる前記ユーザーのプライベートデータに対するアクセスのユーザー制御を提供するプライバシー制御と、
前記無線装置の現在の環境を特徴付けるセンサ信号を供給するセンサと、
前記センサに接続され、前記センサ信号を処理する状況推定エンジンであって、前記プライバシー制御にも接続されており、前記処理によって生成された現在の状況に関する結果を前記アプリケーションプログラムに提供する状況推定エンジンと、
前記プライバシー制御に接続され、前記アプリケーションプログラムに応答し、有用な情報を前記ユーザーに提供する出力装置と、
を有する無線装置。
【請求項２８】
無線装置の現在の環境に適した有用な情報を前記無線装置のユーザーに提供するシステムであって、
前記無線装置からユーザープライバシープロファイルを受信し、アプリケーションプログラムによる前記ユーザーのプライベートデータに対するアクセスのユーザー制御を提供するサーバー内のプライバシー制御と、
前記無線装置の現在の環境を特徴付けるセンサ信号を供給する前記無線装置内のセンサと、
前記無線装置に接続され、前記センサ信号から導出されたセンサ情報を処理する前記サーバー内の状況推定エンジンであって、前記プライバシー制御にも接続されており、前記処理によって生成された現在の状況に関する結果を前記アプリケーションプログラムに提供する状況推定エンジンと、
前記プライバシー制御に接続され、前記アプリケーションプログラムに応答し、有用な情報を前記無線装置に送信する出力装置と、
を有するシステム。
【請求項２９】
無線装置が、該装置の現在の環境に適した有用な情報をそのユーザーに提供できるようにする方法であって、
アプリケーションデータを前記無線装置に供給するプログラムを実行するステップと、
前記無線装置の現在の環境を特徴付けるセンサ信号を受信するステップと、
前記センサ信号と前記アプリケーションデータを状況推定エンジンによって処理するステップと、
前記状況推定エンジンによる処理によって生成された現在の状況に関する結果を出力するステップと、
前記現在の状況に関する結果に応答し、前記ユーザーに有用な情報を提供するステップと、
を有する方法。
【請求項３０】
前記状況推定エンジンによるセンサ信号の処理は、前記ユーザーの無線装置内で稼動するプログラムされた命令として実施される請求項２９記載の方法。
【請求項３１】
前記プログラムを実行するステップは、前記無線装置において実行される請求項３０記載の方法。
【請求項３２】
前記状況推定エンジンによるセンサ信号の処理は、前記ユーザーの無線装置からの信号に応答し、別個のネットワークサーバー内で稼動するプログラムされた命令として実施される請求項２９記載の方法。
【請求項３３】
前記プログラムを実行するステップは、前記ネットワークサーバーに接続されたウェブサーバーにおいて実行される請求項３２記載の方法。
【請求項３４】
無線装置が、該装置の現在の環境に適した有用な情報をそのユーザーに提供できるようにするシステムであって、
プロセッサと；
前記プロセッサに接続されたメモリであって、
アプリケーションデータを前記無線装置に供給するプログラムを実行するステップと、
前記無線装置の現在の環境を特徴付けるセンサ信号を受信するステップと、
前記センサ信号と前記アプリケーションデータを状況推定エンジンによって処理するステップと、
前記状況推定エンジンによる処理によって生成された現在の状況に関する結果を出力するステップと、
前記現在の状況に関する結果に応答し、前記ユーザーに有用な情報を提供するステップと、
を実行するべくプログラムされたメモリと；
を有するシステム。
【請求項３５】
前記状況推定エンジンによる前記センサ信号と前記アプリケーションデータの処理は、前記ユーザーの無線装置内で稼動するプログラムされた命令として実施される請求項３４記載のシステム。
【請求項３６】
前記プログラムを実行するステップは、前記無線装置において実行される請求項３５記載のシステム。
【請求項３７】
前記状況推定エンジンによる前記センサ信号と前記アプリケーションデータの処理は、前記ユーザーの無線装置からの信号に応答し、別個のネットワークサーバー内で稼動するプログラムされた命令として実施される請求項３４記載のシステム。
【請求項３８】
前記プログラムを実行するステップは、前記ネットワークサーバーに接続されたウェブサーバーにおいて実行される請求項３７記載のシステム。
【請求項３９】
無線装置が、該装置の現在の環境に適した有用な情報をそのユーザーに提供できるようにする方法であって、
前記無線装置の現在の環境を特徴付けるセンサ信号を受信するステップと、
前記ユーザーの無線装置内の第１状況推定エンジンによって前記センサ信号を部分的に処理するステップと、
前記部分的に処理されたセンサ信号を別個のネットワークサーバー内の第２状況推定エンジンに送信するステップと、
前記第２状況推定エンジンによって前記信号の処理を完了させるステップと、
前記第２状況推定エンジンによって生成された現在の状況に関する結果を前記無線装置に送信するステップと、
前記現在の状況に関する結果に応答し、前記ユーザーに有用な情報を提供するステップと、
を有する方法。
【請求項４０】
無線装置が、該装置の現在の環境に適した有用な情報をそのユーザーに提供できるようにするシステムであって、
前記無線装置の現在の環境を特徴付けるセンサ信号を受信する無線装置と、
前記センサ信号を部分的に処理する前記ユーザーの無線装置内の第１状況推定エンジンと、
前記無線装置から送信された前記部分的に処理されたセンサ信号を受信し、前記センサ信号の処理を完了させる別個のネットワークサーバー内の第２状況推定エンジンと、
を有し、
前記第２状況推定エンジンは、現在の状況に関する結果を前記第２推定エンジンから前記無線装置に送信し、

前記無線装置は、前記現在の状況に関する結果に応答し、有用な情報を前記ユーザーに提供するシステム。

【請求項４１】

無線装置が、該装置の現在の環境に適した有用な情報をそのユーザーに提供できるようにする方法であって、

前記無線装置の現在の環境を特徴付けるセンサ信号を受信するステップと、

前記ユーザーの無線装置内の第１状況推定エンジンによって前記センサ信号を部分的に処理するステップと、

前記部分的に処理されたセンサ信号を別個のネットワークサーバー内の第２状況推定エンジンに送信するステップと、

前記第２状況推定エンジンによって前記センサ信号の処理を完了させるステップと、

現在の状況に関する結果を前記ネットワークサーバーから第２サーバーに転送するステップと、

前記現在の状況に関する結果に応答し、前記第２サーバーから前記ユーザーの無線装置に、有用な情報を送信するステップと、

を有する方法。

【発明の詳細な説明】

【技術分野】

【０００１】

（関連出願に対する参照）

本出願は、２００１年５月１５日付けの「状況に応じたウェブサービス（Context Sensitive Web Services）」という名称の米国特許出願第０９／８５７，６２８号に対する優先権を主張するものであり、本引用により、その開示内容は本明細書に包含される。

【０００２】

本発明は、インターネットサービスの提供方法に関し、更に詳しくは、インターネットサービスへのモバイル装置によるアクセスの改善に関するものである。

【背景技術】

【０００３】

携帯電話及び無線携帯情報端末（ＰＤＡ）は、ＷＡＰ（Wireless Application Protocol）を使用してインターネットにアクセスすることができる。現在では、ＷＡＰに対応した無線装置により、ヘッドラインニュース、為替レート、スポーツの結果、株式市況、天気予報、多国語熟語辞書、パーソナルオンラインカレンダ、オンライン旅行、又はバンキングサービスなどのインターネットアプリケーションにアクセスしたり、独自の着信メロディをダウンロードすることができる。ＷＡＰに対応した無線装置は、広帯域無線ネットワークを使用し、一般的なテキストに、写真、画像、音声クリップ、又はビデオクリップなどの格段に内容の豊富なコンテンツタイプを組み合わせたマルチメディアメッセージを交換可能である。ＷＡＰに対応した無線装置を使用すれば、無線装置を仮想的な財布として使用し、オンライン上で支払いを済ませることができる。ＷＡＰに対応した無線装置は、オンライン販売業者からの有用且つ有益な広告と取引サービスを提供可能である。更に、ＷＡＰに対応した無線装置により、現在では、対話型のアドベンチャゲーム、クイズ、又はチェスのトーナメントなどのエンターテイメントサービスも提供されている。

【発明の開示】

【発明が解決しようとする課題】

【０００４】

現在、携帯電話や無線ＰＤＡに求められているのは、状況推定技法（context inference techniques）を使用してモバイルユーザーの環境を感知し、これに応答して、感知したユーザー環境に適した有用な情報をユーザーに提供する機能である。状況推定技法に必要となる演算集約的な処理の一部をモバイルユーザーの無線装置からサーバーやインターネット上のウェブサイトに負荷分散（off load）すれば、更に有用であろう。又、モバイルユーザーの個人的な嗜好に関するパーソナルプロファイルをオンラインサーバーやウェブサイトに保持すれば有益であろう。更には、このユーザーのプロファイルに対するオンラインサーバーやウェブサイトからのアクセスを制御する機能をモバイルユーザーに提供することが重要であろう。

【課題を解決するための手段】

【０００５】

状況に応じたウェブサービスに関する本発明は、携帯電話又は無線ＰＤＡが状況推定技法を使用してユーザーの環境を感知し、これに応答して、感知されたユーザー環境に適した有用な情報をユーザーに提供できるようにするものである。

【０００６】

本発明の一態様は、無線装置が当該装置の現在の環境に適した有用な情報をそのユーザーに提供できるようにする方法である。この方法は、無線装置の現在の環境を特徴付けるセンサ信号を受信するステップと；センサ信号を状況推定エンジンによって処理するステップと、状況推定エンジンによる処理によって生成された現在の状況に関する結果を出力するステップと；現在の状況に関する結果に応答して有用な情報をユーザーに提供するステップと；を含んでいる。状況推定エンジンによるセンサ信号の処理は、ユーザーの無線装置内で稼動するプログラムされた命令として実施される。一方、本発明の別の態様においては、この状況推定エンジンによるセンサ信号の処理は、ユーザーの無線装置からの信号に応答し、別個のネットワークサーバー内で稼動するプログラムされた命令として実施される。このサーバーは、ウェブサーバーのファイルにアクセスし、ユーザーの無線装置に対して選択的に転送することができる。このサーバーは、ユーザーのパーソナルプロファイルを保持することができる。

【０００７】

本発明の更なる態様によれば、ユーザーのプライベートデータへのアプリケーションプログラムによるアクセスに対してユーザー制御が提供される。これには、サーバー内のユーザーのプライベートデータへのアプリケーションプログラムによるアクセスに対するユーザー制御の提供も含まれる。更に、これには、ユーザーのプライベートデータへのウェブサーバー内のアプリケーションプログラムによるアクセスに対するユーザー制御の提供も含まれている。

【０００８】

本発明の別の態様によれば、ユーザー制御に応答して現在の状況に関する結果をアプリケーションプログラムに提供し、アプリケーションプログラムから有用な情報を受信する。本発明によれば、ユーザーは、現在の状況に関する結果にアクセスするためのアクセス許可をアプリケーションプログラムに付与することができる。これは、ユーザーの無線装置において、或いはネットワークサーバーにおいて、実行可能である。ネットワークサーバーは、ユーザーの無線装置から受信したユーザーのプライバシープロファイルに応答し、ウェブサーバー内のアプリケーションプログラムによるアクセスを制御することができる。

【０００９】

状況に応じたウェブサービス（context sensitive web service）に関する本発明は、携帯電話又は無線ＰＤＡが状況推定技法を使用してユーザーの環境を感知し、これに応答して、感知されたユーザー環境に適した有用な情報をユーザーに提供できるようにするものである。本発明によれば、状況推定技法に必要となる演算集約的な処理の一部がモバイルユーザーの無線装置からサーバー及びインターネット上のウェブサイトに負荷分散される。状況に応じたウェブサービスに関する本発明によれば、モバイルユーザーの個人的な嗜好に関するパーソナルプロファイルがオンラインサーバー又はウェブサイト内に保持される。そして、このユーザーのプライベートデータに対する無線装置内のアプリケーションプログラムによるアクセスを制御する機能がモバイルユーザーに提供される。又、状況に

応じたウェブサービスに関する本発明によれば、モバイルユーザーには、このユーザーのプロファイルに対するオンラインサーバー又はウェブサイトによるアクセスを制御する機能も提供される。

【００１０】

モバイルユーザーの無線装置は、サードパーティのアプリケーションを含むアプリケーションプログラムに対してモバイルユーザーの状況に関する識別内容を提供する状況推定エンジン（context inference engine）を備えている。通常の無線装置の場合、処理能力と記憶容量が限られているため、状況推定エンジンの演算負荷及び記憶要件を状況データの処理能力を有する状況推定サーバーに分散させる。本発明によれば、モバイルユーザーは、無線装置内のどのアプリケーションプログラムにユーザーのプライベートな状況情報へのアクセスを許可するかを制御することができる。プライバシープロファイル内に保存されているモバイルユーザーの嗜好に基づいて、無線装置内のプライバシー制御ブロックが、プライベートな状況情報へのアプリケーションプログラムによるアクセスを許可したり、取り消したりするのである。この同じプライバシー制御とプライバシープロファイルを状況推定サーバーに拡張することにより、状況推定サーバーに接続されたウェブサーバーにユーザーのプライバシー制御を拡張可能である。従って、本発明によれば、プライベートなユーザーの状況情報に対する制御をモバイルユーザーに提供しつつ、無線装置及びサーバー内において、状況に応じたアプリケーション及びサービスのインフラストラクチャを構築可能である。

【発明を実施するための最良の形態】

【００１１】

本発明を適用する対象は、ＷＡＰ（Wireless Application Protocol）規格を実装した無線電話と無線携帯情報端末（ＰＤＡ）である。図１は、本発明の一実施例のネットワーク図であり、ユーザーのＷＡＰ（Wireless Application Protocol）対応携帯型無線装置１００、ＷＡＰプロトコルゲートウェイ１２０、及びサーバー１４０間の関係の一例を示している。ユーザーのＷＡＰ対応携帯型無線装置１００は、無線携帯電話、ポケットベル、双方向無線送受信機（two-way radio）、スマートフォン、パーソナルコミュニケータ、又はこれらに類似のものであってよい。ユーザーのＷＡＰ対応携帯型無線装置１００は、デックと呼ばれる小さなファイルにアクセスするが、このデックは、当該装置のマイクロブラウザ１０２の表示領域内に十分フィットする小さなカードと呼ばれる複数の小さな頁から構成されている。このマイクロブラウザ１０２の小さなサイズと小さなファイルサイズは、携帯型無線装置１００のメモリ及び無線ネットワーク１１６の帯域幅に伴う厳しい制約に対応したものである。カードは、小さな画面とキーボードなしの片手によるナビゲーション用に特に考案されたＷＭＬ（Wireless Markup Language）で作成される。このＷＭＬ言語は、携帯電話のマイクロブラウザ１０２上の２行分のテキストディスプレイからスマートフォンやパーソナルコミュニケータが備える大きなＬＣＤ画面までをカバーする拡張性を備えている。ＷＭＬ言語で作成されたカードには、ＷＭＬＳｃｒｉｐｔで作成されたプログラムを含めることができる。ＷＭＬＳｃｒｉｐｔは、ＪａｖａＳｃｒｉｐｔに類似しているが、その他のスクリプト言語が備えている多くの不必要な機能を省いているため、装置１００に要求されるメモリとＣＰＵの処理能力は最小限のものになっている。

【００１２】

Nokia WAP Client Version 2.0は、無線装置１００上でＷＡＰクライアント１０８を実装するのに必要なコンポーネントを含むソフトウェアプロダクトである。これらのコンポーネントには、ＷＭＬ（Wireless Markup Language）ブラウザ、ＷＭＬScriptエンジン、プッシュサブシステム、及び無線プロトコルスタックが含まれている。このNokia WAP Clientは、携帯電話や無線ＰＤＡなどの無線装置へのポーティング及び組み込みが可能なソースコードプロダクトである。無線装置１００内に保存されているアプリケーションプログラム１０６は、ＷＡＰクライアント１０８とやり取りして様々な通信アプリケーションを実装する。尚、Nokia WAP Client Version 2.0の詳細については、www.nokia.com/corporate/wapに所在する「Nokia WAP Client Version 2.0:製品概説書（Product Overview）」（ノキア・インターネット・コミュニケーションズ社（Nokia Internet Communications）、２０００年）という名称のオンラインペーパーを参照されたい。

【００１３】

ＷＡＰクライアント１０８には、サーバー及び無線クライアントの認証とデジタル署名に必要なインフラストラクチャ及び手順を提供する無線ＰＫＩ（Public Key infrastructure）機能が含まれている。無線ＰＫＩとは、モバイルトランザクションに関係する各当事者に関連付けられたパブリック／プライベートキーペアを利用する証明書に基づいたシステムである。ＷＩＭ（Wireless Identity Module）は、ＷＡＰクライアント１０８のセキュリティトークン機能であり、ユーザー認証とデジタル署名に必要なパブリック及びプライベートキーとサービス証明書などのセキュリティ機能が含まれている。又、ＷＩＭは、暗号化処理を実行しメッセージの暗号化／復号を行う能力をも備えている。

【００１４】

図１の無線装置１００には、モバイルユーザーの周辺条件を感知する複数のセンサも具備されている。図示のセンサには、位置センサ１２２、接触センサ１２４、オーディオセンサ１２５、コンパスセンサ１２６、周辺光センサ１２８、周辺温度センサ１３２、及び３軸加速度センサ１３４が含まれている。オーディオセンサ１２５は、例えば、音声又は環境音響を検出可能なマイクであってよい。位置センサは、例えば、装置に内蔵されたＧＰＳ受信機であってよい。或いは、この位置センサは、例えば、「移動局測位システム（Mobile Station Positioning System）」という名称のノキア社（Nokia）の欧州特許第0,767,594A2号明細書に記述されているものなどのラジオビーコン、基地局、又はアクセスポイントのネットワークを利用した無線装置の位置を判定するラジオビーコン三角測量センサであってもよい。これらのセンサは、後述するように、現在の状況を推定するべく無線装置１００がサンプリングする入力を供給する。

【００１５】

ＷＡＰプロトコルゲートウェイ１２０は、インターネット１３０と無線ネットワーク１１６をリンクしている。このＷＡＰプロトコルゲートウェイ１２０には、無線装置１００に対する安全なインターネット接続の提供を支援する無線ＰＫＩ（Public Key infrastructure）が含まれている。ＷＡＰプロトコルゲートウェイ１２０により、ＷＡＰ対応無線装置１００は、ヘッドラインニュース、為替レート、スポーツの結果、株式市況、オンライン旅行、又やバンキングサービスにアクセスしたり、独自の着信メロディをダウンロードすることができる。

【００１６】

ユーザーのＷＡＰ対応携帯型無線装置１００は、無線塔１１４と通信し、最高数キロメートルの距離においてメッセージを交換することができる。ＷＡＰ規格がサポートしている無線ネットワーク１１６のタイプには、ＣＤＰＤ（Cellular Digital Packet Data）、ＣＤＭＡ（Code-Division Multiple Access）、ＧＳＭ（Global System for Mobile Communications）、ＴＤＭＡ（Time Division Multiple Access）、GPRS、3G-Broadband、又はこれらに類似のものが含まれる。

【００１７】

ユーザーのＷＡＰ対応無線装置（クライアント）１００とサーバー１４０間におけるＷＡＰプロトコルゲートウェイ１２０を介した通信の全体的なプロセスは、次のように、ＨＴＴＰ（HyperText Transfer Protocol）、即ち、ワールドワイドウェブプロトコルを使用してインターネット上でウェブ頁をサービスする方法と類似している。

【００１８】

（１）ユーザーは、サーバー１４０のＵＲＬ（Uniform Resource Locator）に関連付けられたユーザー装置（１００）上の電話キーを押す。

【００１９】

（２）ユーザー装置（１００）は、ＷＡＰプロトコルを使用し、無線塔１１４及び無線ネットワーク１１６を介してＵＲＬをゲートウェイ１２０に送信する。

【００２０】

（３）ゲートウェイ１２０は、このＷＡＰ要求をＨＴＴＰ要求に変換し、それをＴＣＰ／ＩＰ（Transmission Control Protocol/Internet Protocol）インターフェイスにより、インターネット１３０を介してサーバー１４０に送信する。

【００２１】

（４）サーバー１４０は、インターネットを介して受信されるその他のＨＴＴＰ要求とまったく同様に、この要求を取り扱う。サーバー１４０は、例えば、ＣＧＩ（Common Gateway Interface）プログラム、Ｊａｖａサーブレット、又はこれらに類似のものなどによって作成された標準的なサーバープログラムを使用し、

WMLデック又はＨＴＭＬ（HyperTest Markup Language）頁のいずれかをゲートウェイ１２０に返す。

【００２２】

（５）ゲートウェイ１２０は、ユーザー装置（１００）に代わって、このサーバー１４０からの応答を受信する。この応答がＨＴＭＬ頁の場合には、必要に応じて、WMLに符号変換される。そして、このWML及びWMLＳｃｒｉｐｔコードは、バイトコードに符号化された後に、ユーザー装置１００に送信される。

【００２３】

（６）ユーザー装置１００は、このWMLバイトコード化された応答を受信し、ユーザーに対して、マイクロブラウザ１０２上のデックに第１カードを表示する。

【００２４】

図１において、プロトコルゲートウェイ１２０は、５つの異なるレイヤに編成されたＷＡＰプロトコルスタックを含んでいる。アプリケーションレイヤは、無線アプリケーション環境であり、携帯型アプリケーション及びサービスを実行する。セッションレイヤは、無線セッションプロトコルであり、クライアント／サーバーアプリケーション間においてコンテンツを組織的に交換する方法を提供する。トランザクションレイヤは、無線トランザクションプロトコルであり、信頼性の高いトランザクションを実行する方法を提供する。セキュリティレイヤは、無線トランスポートレイヤのセキュリティ機能であり、アプリケーション間における認証、プライバシー、及び安全な接続を提供する。トランスポートレイヤは、無線データグラムプロトコルであり、ＣＤＰＤ、ＣＤＭＡ、ＧＳＭなどの様々な無線ネットワークプロトコルの固有要件から上位レイヤを保護している。尚、ＷＡＰ規格及びＷＡＰプロトコルスタックに関する更なる情報については、２０００年にロックス・プレス社（Wrox Press Ltd.）から出版されたチャールズ・アレハート（Charles Arehart）他による「プロのＷＡＰ（Professional WAP）」という名称の書籍（ISBN 1-861004-04-1）を参照されたい。

【００２５】

図１において、ユーザーの携帯型無線装置１００には、『状況に応じたサービス』メニューを表示するマイクロブラウザ１０２が含まれており、これにより、ユーザーは、表示されたカードをナビゲートし、アプリケーションプログラム１０６によってプログラムされたオプションを選択することができる。又、ユーザーの装置１００には、前述のＷＡＰクライアントプログラム１０８も含まれている。

【００２６】

図１のマイクロブラウザ１０２に表示されている『状況に応じたサービス』メニューは、図２及び図２Ａに示されているアプリケーションプログラム１０６の制御下において、ＷＡＰクライアントプログラム１０８によってレンダリングされる。この「状況に応じたサービス」メニューにより、ユーザーは、（Ａ）「プライバシー機能の更新」、又は（Ｂ）『アプリケーションの実行」といういずれかのセッションタイプを選択可能である。そして、ユーザーが「プライバシー機能の更新」セッションタイプを選択した場合には、図１の「状況に応じたサービス」メニューは、ユーザーに対して「プライバシー機能の更新」サブメニューを提示し、ユーザーは、このサブメニューから次のオプションを選択することができる。

【００２７】

（Ａ）プライバシー機能の更新

（１）あなたのプライバシープロファイルの更新

（２）あなたのパーソナルデータの更新

（３）プログラムの認証

【００２８】

オプション（１）の「あなたのプライバシープロファイルの更新」を選択すると、図１Ａに示されている第２のサブメニューが表示され、これは次のオプションを備えている。

【００２９】

（１）あなたのプライバシープロファイルの更新

（ａ）許可リストへのローカルプログラムの追加

（ｂ）リストからのローカルプログラムの削除

（ｃ）許可リストへのサーバープログラムの追加

（ｄ）リストからのサーバープログラムの削除

（ｅ）許可リストへのネットワークプログラムの追加

（ｆ）リストからのネットワークプログラムの削除

【００３０】

オプション（２）「あなたのパーソナルデータの更新」を選択すると、図１Ａに示されている別のサブメニューが表示され、これは次のオプションを備えている。

【００３１】

（２）あなたのパーソナルデータの更新

（ａ）サーバーデータベースの更新

（ｂ）ネットワークデータベースの更新

【００３２】

オプション（３）の「プログラムの認証」を選択すると、図１Ｂに示されている別のサブメニューが表示され、これは次のオプションを備えている。

【００３３】

（３）プログラムの認証

（ａ）プログラムのパブリックキー証明書の要求

（ｂ）証明書の署名の検証

（ｃ）有効期間の検証

（ｄ）取り消し状態の検証

（ｅ）認証局が信用リストに含まれているかどうかのチェック

（ｆ）プログラムへの認証フラグの設定

【００３４】

この「プログラムの認証」オプションにより、図２の無線装置１００のプライバシー制御１５０が呼び出される。信頼できる機関によるアプリケーションプログラムＡ、Ｂ、Ｘ、又はＹの妥当性の検証が完了している場合には、その信頼できる機関により、アプリケーションプログラムに対して算出されたＭＡＣ（message authentication code）に関するデジタル証明書が発行されており、プライバシー制御１５０はその証明書をチェックすることができる。プライバシー制御１５０が、そのデジタル証明書を発行した信頼できる機関を信頼している場合には、そのアプリケーションプログラムの認証は簡単である。

【００３５】

プログラムのデジタル署名を検証し、そのアプリケーションプログラムがユーザーのプライベートデータの完全性又は信頼性を損なわないと判断した場合には、ユーザーは、そのプログラムを登録することができる。この「登録」とは、ユーザーの無線装置の現在の状況及び／又はユーザーのプライベートデータのその他の部分に対してアクセスするためのアクセス許可をユーザーがプログラムに付与することを意味している。ユーザーが付与可能な許可には、（ａ）『いつアクセス可能か』、及び（ｂ）「どのデータにアクセス可能か」という２つのカテゴリにおいて複数レベルが存在する。

【００３６】

オプション（４）の「プログラムの登録」を選択すると、図１Ｂに示されている別のサブメニューが表示され、これは次のオプションを備えている。

【００３７】

（４）プログラムの登録

（ａ）いつアクセス可能か

（ｂ）どのデータにアクセス可能か

【００３８】

第１カテゴリである（ａ）「いつアクセス可能か」の場合、許可の最高レベルは、「通知なしにいつでもアクセス可能」というものである。一方、このカテゴリにおける許可の最低レベルは、「指定された時点又は指定された条件であり、且つユーザーに通知しユーザーによる個別認可の後でのみアクセス可能」というものである。第２のカテゴリの（ｂ）「どのデータにアクセス可能か」の場合には、許可の最高レベルは、「現在の状況情報、ユーザーが入力したパーソナルデータ、ユーザーのインターネット利用履歴データ、ユーザーのインターネットクッキーデータ、及びユーザーのアプリケーションプログラム使用状況データを含むユーザーのプライベートデータ内のデータセットに対する無制限のアクセス」

である。このカテゴリにおける許可の最低レベルは、「ユーザーに通知しユーザーによる個別認可の後でのみデータにアクセス可能」というものである。ユーザーは、最高と最低の間のどのような許可レベルでも設定可能であり、それを登録の基準にすることができる。ユーザーは、ユーザーが署名しアプリケーションプログラムに添付するデジタル証明書の中に、この登録条件を含めることができる。要求するアクセスイベントの前に、この登録証明書をプログラムからプライバシー制御１５０に対して提示することにより、プライバシー制御１５０はプログラムの登録状態を自動的に検証可能である。この登録証明書は、次のように作成することができる。

【００３９】

プライバシー制御１５０は、ＭＡＣ（message authentication code）及び独自のデジタル署名を算出し、受け入れ可能なアプリケーションプログラムＡ、Ｂ、Ｘ、又はＹに対して証明書として添付する。プライバシー制御１５０は、このデジタル証明書の中に登録条件を含めることができる。この結果、プライバシー制御１５０は、プログラムがユーザーのプライベートデータへのアクセスを要求した際に、ＭＡＣ及び独自のデジタル署名を自動的にチェックし、プログラムが変更されていないことを検証することができる。又、プライバシー制御１５０は、プログラムの登録状態を自動的に検証することもできる。即ち、プライバシー制御１５０は、アプリケーションプログラムＡ、Ｂ、Ｘ、又はＹの全体（又はその一部）及び登録条件のハッシュ値を算出した後に、このハッシュ値からＭＡＣ（message authentication code）を形成することにより、これを実現する。次いで、プライバシー制御（１５０）は、自分のＰＫＩプライベートキーを使用してＭＡＣ（message authentication code）にデジタル署名する。そして、これら登録条件、ＭＡＣ、及びプライバシー制御のデジタル署名が、アプリケーションプログラムＡ、Ｂ、Ｘ、又はＹに登録証明書として添付されるのである。

【００４０】

この結果、プライバシー制御１５０は、アプリケーションプログラムＡ、Ｂ、Ｘ、又はＹがユーザーの状況データ又はプライベートデータへのアクセスを要求した際に、提示されたＭＡＣが算出されたＭＡＣと一致すること、並びに提示さ

ー１６０からのアクセス要求に対するプライバシーチェックを自動的に処理可能である。即ち、ウェブサーバー１６０内のアプリケーションプログラムがネットワークサーバー１４０内又は無線装置１００内のユーザープライベートデータへのアクセスを要求すると、ネットワークサーバー１４０内のプライバシー制御１６４は、ＭＡＣ及び独自のデジタル署名をチェックしてアプリケーションプログラムが変更されていないことを検証できるよう、そのウェブサーバー１６０内のアプリケーションプログラムに対して登録証明書の提示を要求する。この結果、プライバシー制御１６４は、登録条件に従い、そのウェブサーバー１６０内のアプリケーションプログラムに対してアクセス許可を自動的に付与することができる。

【００４３】

ユーザーが（Ｂ）「アプリケーションの実行」というセッションタイプを選択した場合には、図１Ｃの「状況に応じたサービス」メニューは、ユーザーに対して「アプリケーションの実行」サブメニューを提示し、これは次のオプションを備えている。

【００４４】

（１）メッセージング
（ａ）マルチメディアメッセージの交換
（２）モバイルコマース
（ａ）パーソナルオンラインカレンダ
（ｂ）為替レート
（ｃ）バンキングサービス
（ｄ）仮想財布によるオンライン上での支払い
（ｅ）有用且つ有益な広告
（ｆ）オンライン販売業者との取引サービス

【００４５】

図１Ｄの「状況に応じたサービス」メニューは、ユーザーに対して「アプリケーションの実行」サブメニューを提示しており、これは次のオプションを備えている。

れたデジタル署名が本物であることをチェックできるよう、アプリケーションプログラムに対して登録証明書の提示を要求する。そして、プライバシー制御１５０は、その登録条件に従って、アプリケーションプログラムに対してアクセス許可を自動的に付与するのである。

【００４１】

ＭＡＣ（message authentication code）を生成及び評価しデータの完全性を保証する方法については、２０００年にジョン・ワイリー・アンド・サンズ社（John Wiley and Sons）から出版されたステファン・トーマス（Stephen Thomas）による「ＳＳＬとＴＬＳ（SSL and TLS）」という名称の書籍に記述されている。メッセージ認証用のアルゴリズムの例としては、ＲＳＡのＭＤ５（Message Digest）及びＳＨＡ（Secure Hash Algorithm）の２つを挙げることができ、これらについては、いずれも前述のステファン・トーマスによる書籍に記述されている。データの完全性を確保する方法の更なる詳細については、１９９６年にジョン・ワイリー・アンド・サンズ社（John Wiley and Sons）から出版されたブルース・シュナイア（Bruce Schneier）による「応用暗号法ー第２版（Applied Cryptography-2nd Edition）」という名称の書籍を参照されたい。デジタル署名を生成及び評価してデジタルプログラムのソースを保証する方法については、１９９７年にアディソン・ウェスリー社（Addison Wesley）から出版されたリチャード　Ｅ．スミス（Richard E. Smith）による「インターネット暗号法（Internet Cryptography）」という名称の書籍に記述されている。

【００４２】

前述の無線装置１００内のプライバシー制御１５０に関する説明内容は、図２Ａのネットワークサーバー１４０内のプライバシー制御１６４に対しても同様に適用される。ネットワークサーバー１４０内のプライバシー制御１６４は、ＭＡＣ（message authentication code）と独自のデジタル署名を算出し、登録条件と共に、ウェブサーバー１６０内の受け入れ可能なアプリケーションプログラムに対して登録証明書として添付することができる。プライバシー制御１６４は、無線装置１００のプライバシープロファイル１５２のキャッシュされた複写１４４を備えている。この結果、ネットワークサーバー１４０において、ウェブサーバ

【００４６】

（３）エンターテイメント
（ａ）ヘッドラインニュース
（ｂ）スポーツの結果
（ｃ）株式市況
（ｄ）天気予報
（ｅ）多国語熟語辞書
（ｆ）オンライン旅行
（ｇ）独自の着信メロディのダウンロード
（ｈ）対話型ゲーム

【００４７】

この「アプリケーションの実行」オプションにより、図２の無線装置１００のアプリケーションプログラムＡ、Ｂ、Ｘ、又はＹの中の１つが呼び出される。

【００４８】

図２は、無線装置１００の機能ブロックダイアグラムであり、その様々なコンポーネント及びプログラムが示されている。無線装置１００は、ダウンロードするか或いはファームウェアの状態にある状況に応じたアプリケーションＡ、Ｂ、Ｘ、及びＹを備えている。この無線装置１００は、センサ入力の初期サンプリング及びデジタル化の際には、ネットワーク内の外部機能を利用する必要はない。このセンサ入力からサンプリングされデジタル化される値は、位置メタデータ１２２’、接触メタデータ１２４’、オーディオメタデータ１２５’、コンパスメタデータ１２６’、周辺光メタデータ１２８’、周辺温度メタデータ１３２’、及び３軸加速度メタデータ１３４’である。これらのセンサ入力からサンプリングされデジタル化された値は、メタデータベクトル１３８内に読み込まれる。

【００４９】

図２は、キーパッド１０４、送受信機２０６、センサインターフェイス２０８、中央プロセッサ２１０、及びディスプレイ２１２にバス２０４によって接続された無線装置１００のメモリ２０２を示している。このメモリ２０２は、プロセッサ２１０によって実行された際に、本発明の方法を実行する実行形式命令のシー

ケンスであるプログラムを保存している。即ち、メモリ２０２は、ＷＡＰクライアントプログラム１０８、状況推定エンジン１３６、プライバシー制御１５０、プライバシープロファイル１５２、状況識別ＡＰＩ１５４、動作／ジェスチャＡＰＩ１５６、位置ＡＰＩ１５８、及びその他ＡＰＩ１６２を保存している。状況推定エンジン１３６は、メタデータベクトル１３８を処理して現在の状況を生成する。メモリ２０２内に保存されているアプリケーションプログラム１０６には、ソフトウェアシステムＳＳ１の一部であるアプリケーションプログラムＡ及びＢと、実行環境「Ｅｘｅｃ．Ｅｎｖ．」に格納されているアプリケーションプログラムＸ及びＹと、が含まれている。

【００５０】

無線装置１００に十分な演算能力と記憶容量が提供されておれば、現在の状況に関する推定結果の生成という最終目的を完了する時点まで、状況推定エンジン１３６によってメタデータベクトル１３８の処理を継続実行可能である。しかしながら、演算の途中で、ネットワークサーバー１４０に提供されている処理能力又は記憶容量を状況推定エンジン１３６が必要とする場合には、無線装置１００から図２Ａのネットワークサーバー１４０内の状況推定エンジン１４２にメタデータベクトル１３８が送信される。そして、ネットワークサーバー１４０内の状況推定エンジン１４２は、必要な処理をメタデータベクトル１３８に対して実行した後に、現在の状況に関する推定結果を完成させるべく、処理結果を無線装置１００内の状況推定エンジン１３５に返す。或いは、この代わりに、ネットワークサーバー１４０内の状況推定エンジン１４２は、必要な処理をすべて完了させた後に、生成された現在の状況に関する推定結果を無線装置１００に返す。

【００５１】

図２には、状況の識別をサポートする無線装置のアーキテクチャが示されている。この状況の識別は、図１に示されているハンドセット内に物理的に位置している様々なタイプのセンサから受信したセンサ情報の上に構築されるものである。図示のセンサには、位置センサ１２２、接触センサ１２４、オーディオセンサ１２５、コンパスセンサ１２６、周辺光センサ１２８、周辺温度センサ１３２、及び３軸加速度センサ１３４が含まれている。これらのセンサは、アクセサリのような電話機カバーの内部やブルートゥース対応装置などの無線アクセサリの内部に配置することも可能である。又、センサは、ユーザーの部屋や車両の内部などの環境内に配置することもできる。又、状況識別サービスにおいては、これらのセンサデータと共に、電話機の使用時間やその他の入手可能な情報を使用することも可能である。

【００５２】

図２には、センサ１２２、１２４、１２５、１２６、１２８、１３２、及び１３４から受信され、状況推測エンジン１３６によって処理されるセンサデータが示されている。無線装置１００で稼動中のアプリケーションプログラムＡ、Ｂ、Ｘ、又はＹは、任意選択により、現在の状況に対する要求と共に、アプリケーションデータを状況推定エンジン１３６に提供することも可能である。状況推定エンジン１３６も、任意選択により、これらセンサ信号及びアプリケーションデータを処理し、現在の状況を生成可能である。そして、状況推定エンジン１３６は、様々なＡＰＩ１５４、１５６、１５８、及び１６２を介して、現在の状況をアプリケーションＡ、Ｂ、Ｘ、及びＹに提供する。アプリケーションプログラムは、現在の状況又は状況の変化を受信するべく、自分自身をアプリケーションプログラムインターフェイス１５４に登録することができる。この結果、そのアプリケーションプログラムは、状況を感知できるようになる。

【００５３】

図２には、無線装置１００の第１ソフトウェアシステムＳＳ１において稼動する「ネイティブ」のアプリケーションプログラムＡ及びＢが示されている。本明細書において使用されているこの「ソフトウェアシステム」という用語は、実行能力を有するあらゆる環境を意味している。第１ソフトウェアシステムは、ＮＯＳ、ＩＳＡ、ＥＰＯＣ、ＪＡＶＡ（登録商標）、又はＷＡＰなどのプロプライエタリなものや市販されているリアルタイムオペレーションシステムに基づいたものであってよい。サードパーティアプリケーションプログラムＸ及びは実行環境において稼動する。この実行環境においては、ＡＰＩに対するアクセスなどのアプリケーションに提供されるシステム機能を制限（固定又は動的な動作）することができる。

【００５４】

図２には、モバイルユーザーのプライバシー制御機能が示されている。このプライバシー制御機能により、ユーザーは、状況推定エンジン１３６によって生成された現在の状況情報を利用するべく、どのアプリケーションプログラムに状況識別ＡＰＩ１５４へのアクセスを許可するかを指定することができる。状況推定エンジン１３６にアクセスするためのアプリケーションプログラムＡ、Ｂ、Ｘ、及びＹによる要求又は登録は、すべて最初にプライバシー制御ブロック１５０を通過しなければならない。プライバシー制御ブロック１５０は、プライバシープロファイル１５２内に保存されているユーザーのセキュリティデータチェックを使用して要求元のアプリケーションプログラムにアクセス権を付与する。ユーザーは、ユーザーインターフェイスを介してユーザーが入力するユーザーセキュリティデータにより、このアクセス権の付与を制御する。ユーザーセキュリティデータには、許可リスト１５５、ＰＫＩ（Public Key Infrastructure）証明書１５７、ＰＫＩによって信頼することができる機関の信用リスト１５９、及びＰＫＩ手順によって認証済みのアプリケーションプログラムにユーザーが設定したフラグであるデータセット１６１が含まれている。ユーザーは、図１Ａ及び図１Ｂに示されている無線装置１００が表示する「プライバシー機能の更新」サブメニューにより、このユーザーセキュリティデータを更新することができる。アクセスは、デジタル署名に基づいてアプリケーションプログラムに許可されるが、これは、システムアプリケーションの一部、或いは当技術分野における周知のその他の手段によって実行される。又、プライバシー制御１５０に対して、別個のシステム全体を対象としたプライバシーユーザーインターフェイスを提供することも可能であり、モバイルユーザーは、これを使用してプライバシーポリシーを設定し、アプリケーションプログラムがユーザーのプライベートな状況識別情報を受信するべく登録しようとしていることに関する警告を受信可能である。プライバシー制御１５０及びプライバシープロファイル１５２により、モバイルユーザーは、アクセスの許可、拒否、又は取り消しを行ったり、時間を限定してアクセスを許可したり、或いは、ユーザーがアクセスを許可する前に、アプリケーションプログラムが常に登録を要求するように求めることができる。

【００５５】

図２において、無線装置１００内の状況推定エンジン１３６は、その無線装置がユーザーによって配置されている場所に基づいたすべてのセンサ入力をもとにして推定を実行する。推定対象の装置１００の現在の状況は、例えば、特定のセンサの組から値が特定の範囲内にある信号の特定の組み合わせが入力された場合に、「ユーザーのポケットの中に位置している」と判断される。一例として、状況推定エンジン１３６による現在の状況の推定結果は、ＸＭＬ言語により、次のように表現可能である。

【００５６】

<Context Inference Engine in Device>
<device placement>ポケット</device placement>
<User Interface state>スリープモード</User Interface state>
<device location>ビル１の２階のエレベータ５の中</device location>
<API active actions>３階の３２２号室で会議が始まる</API active actions>
</Context Inference Engine in Device>

【００５７】

無線装置１００内の状況推定エンジン１３６は、いくつかの方法により、状況推定プロセスを実行可能である。分析対象のそれぞれの環境条件又は状況に適した重要度の相対値により、それぞれのセンサからの入力情報を重み付けすることができる。各センサは、その独自の重み付け値を備えている。或いは、この代わりに、それぞれの環境条件用の各センサの重み付け値を、例えば、人工ニューラルネットワーク（ＡＮＮ）、自己組織化マップ（ＳＯＭ）、意思決定樹状図、ファジー規則に基づいたシステム、或いは、隠れ（Hidden）マルコフモデル（ＨＭＭ）などのモデルに基づいたシステムを使用し、トレーニングセッションから学習することも可能である。更には、アプリケーションに応じて、複数の代替方法の組み合わせを使用することもできる。

【００５８】

状況推定エンジン１３６は、適応的且つ継続的な学習法により、その重みを継続

的に適合させることができ、その際には、ユーザーは、無線装置１００に対して新しい環境条件について教え、それらに名前を付ける。例えば、隠れマルコフモデル（ＨＭＭ）を使用して、状況推定エンジン１３６用の適応的且つ継続的な学習法を実装可能である。この代わりに、既知の場面と比較することにより、変化した場面を自発的に認識するように無線装置１００をプログラムすることもできる。ユーザーは、ニューラルネットワークの適応的且つ自動的な学習能力を使用し、無線装置に対して新しい環境条件について教え、それらに名前を付けることができる。適応的且つ継続的な学習法は演算集約的であり、後述するように、無線装置１００を支援するネットワークサーバー１４０上に配置するのに適当な候補である。

【００５９】

状況推定の分野においては、自動パターン認識の原理が様々なタイプのセンサ入力に適用されている。音声信号の処理には音声認識が適用されており、手の力及び加速度計信号の処理には手書き認識が適用されている。ロボット工学の分野においては、デジタル化された静止画及び動画の処理に画像認識が適用され、レーザー及びソナー測距機信号の処理に機械的な位置認識が適用されると共に、慣性、加速度、及び方位信号の処理に機械的動作認識が適用されている。義肢装置の分野においては、触覚センサ信号の処理に接触認識が適用されている。医学の分野では、伝統的な脈拍、呼吸速度、及び体温信号と共に、生体電場信号を処理することにより、自動診断プログラムが様々な病状を認識している。これらの様々な信号認識プロセスは、サンプリングした信号とそれらの信号の統計的なモデルを同等視する初期トレーニングステップを実施する、という共通的な特徴を備えている。

【００６０】

これらの様々なセンサ入力を自動的にパターン認識する原理について、音声パターンを認識する技法を使用し以下に例示することとする。音声認識に使用されている一般的な技法は、隠れマルコフモデル（ＨＭＭ）である。この「隠れ」という用語は、音声信号の基礎をなしている確率論的であって直接的に観測できないイベントを意味している。ＨＭＭ音声認識システムにおいては、通常、トレーニングサンプルの組から推定されたパラメータを備える音声セグメントの統計モデルである音素を構成して使用する。音声セグメントの適切な統計モデルを鎖状連結又はリンクすることにより、単語のモデルを作成する。これらの統計モデルは、認識対象の未知の音声信号とマッチングするための基準として機能する。

【００６１】

未知の音声信号を認識するには、発話者が発した音素をサンプリングしデジタル化することが必要になる。次いで、これらのデジタル化された音素を処理してメタデータにする。そして、このメタデータを音素の基準である統計モデルと比較する。この結果、最もよくマッチしたものが音声認識の推定結果となる。

【００６２】

認識は、入力音声信号用の単語モデルの組において最も可能性の高い経路を検出するステップによって構成されている。ＨＭＭ音声認識デコードシステムは、最初に、反復プロセスによってトレーニングする必要がある。即ち、システムに、トレーニングサンプル、即ち、特定の発話者の音声による単語を学習させなければならないのである。トレーニング用の単語を分析し、フレーム化された音響パラメータのシーケンス、即ち、統計モデルを生成する。このトレーニング用単語の単語モデルの組における最も可能性が高い経路が正しいトレーニング用単語を認識するようになった場合に、その認識は、有効な、即ち、「優れた」ものとなる。

【００６３】

隠れマルコフモデルの原理について記述した有用な参照資料としては、Ｌ.Ｒ.ラビナー（Ｌ. Ｒ. Rabiner）による「隠れマルコフモデルに関するチュートリアルと音声認識における選択されたアプリケーション（A tutorial on hidden Markov models and selected applications in speech recognition）」（Proceedings of the IEEE、１９８９年、第７７巻、第２号、２５７～２８６頁）、Ｌ.Ｒ.ラビナー（Ｌ. Ｒ. Rabiner）及びB.H.チュアン（B. H. Juang）による「隠れマルコフモデル入門（An introduction to hidden Markov models）」（IEEE ASSP Magazine、１９８６年１月、４～１５頁）、１９９４年にアディソン・ウェスリー社（Addison Wesley）から出版されたアンドレアスＳ．ワイゲント（Andreas S. Weigend）及びネイルＡ．ガーシェンフェルト（Neil A. Gershenfeld）監修による「時系列予測：未来の予測と過去の理解（Time Series Prediction:Forecasting the Future and Understanding the Past）」のアンドリューＭ．フレーザー（Andrew M. Fraser）及びアレクシス・ディミトリアディス（Alexis Dimitriadis）による『混合状態を有する隠れマルコフモデルを使用した確率密度の予測（Forecasting Probability Densities by Using Hidden markov Models with Mixed States）』、及び１９９３年にマサチューセッツ州ケンブリッジに所在するＭＩＴプレス社（MIT Press, Cambridge, Massachusetts）から出版されたユージン・チャーニアック（Eugene Charniak）による「統計的な言語学習（Statistical Language Learning）」がある。

【００６４】

隠れマルコフモデルを音声認識以外にどのように拡張可能であるかを示すべく、次に、接触認識の例について説明する。接触認識のトレーニングステップにおいて、例えば、サンドペーパーなどの粗い組織に触覚トランスデューサを接触させることにより、触覚センサ信号を入力する。そして、この触覚センサ信号を入力信号の統計モデルに変換し、この統計モデルを「粗い＿組織」（rough_texture）というハンドルでコンピュータメモリに基準として保存する。次いで、「粗い＿組織」のモデルに含まれているセンサ信号の範囲を拡張するべく、サンドペーパーに接触させる方向又は圧力がそれぞれ異なる複数のトレーニングセッションを実施し、これによって、統計モデルの複数の異なるサンプルが生成される。そして、これらの統計モデルのサンプルの組を「粗い＿組織」というハンドルで基準として保存する。次いで、その他のトレーニングセッションをガラスなどの滑らかな組織によって実施する。触覚トランスデューサを滑らかな組織に接触させることによって入力される触覚センサ信号を入力信号の統計的モデルに変換し、「滑らかな＿組織」（smooth_texture）というハンドルで基準として保存する。後に、認識モードにおいて、触覚トランスデューサを未知の物体に接触させ、サンプルの触覚センサ信号を生成する。未知の接触信号を認識するには、接触トランスデューサ信号のサンプリングとデジタル化が必要となる。次いで、これらのデジタル化されたセンサ信号を処理してメタデータを生成する。そして、このメタデータを「粗い＿組織」及び「滑らかな＿組織」の基準統計モデルと比較する。この結果、最もよく一致したものが接触認識の推定結果となる。

【００６５】

複数のタイプのセンサを組み合わせることにより、それらの信号を合成サンプリングイベントを特徴付ける入力メタデータに合成可能である。隠れマルコフモデル（ＨＭＭ）の原理を使用し、この合成サンプリングイベントを認識することができる。無線装置１００のユーザーの健康及び疲労の状態が、この合成サンプリングイベントの一例である。無線装置１００は、例えば、無線装置１００を掴んでいるユーザーの手の力と脈拍に応答して触覚センサ信号を出力する触覚トランスデューサを備えることができる。又、無線装置１００は、無線装置１００を掴んでいるユーザーに応答し、体温信号を出力する温度センサを備えることもできる。隠れマルコフモデル（ＨＭＭ）を使用し、サンプリングイベントの結果生成される手の力及び温度センサ信号の組み合わせを特徴付ける力／温度入力メタデータベクトルを認識することができる。尚、この例における合成サンプリングイベントには、一定期間にわたってユーザーの脈拍を力センサが信号変換できるよう、期間を設定可能である。

【００６６】

トレーニングステップにおいて、ユーザーが良好な健康状態にあり普通に休息している際に、触覚センサ信号及び力センサ信号を出力させる。そして、これらの触覚センサ信号及び力センサ信号を力／温度入力メタデータベクトルに合成し、このメタデータベクトルを入力信号の統計モデルに変換する。次いで、この統計的モデルを無線装置１００のコンピュータメモリに基準として「良好な＿健康状態＿普通に＿休息している」（good_health_resting_normally）というハンドルで保存する。次いで、異なる健康及び疲労状態にあるユーザーを対象にして、その他のトレーニングセッションを実施する。例えば、ユーザーが職場で夜遅くに働いている際に、無線装置１００をトレーニングする。無線装置１００を保持することによって生成される触覚センサ信号及び力センサ信号を『健康状態は良好であるが疲労した状態にあるユーザー」の力／温度入力メタデータベクトルとして合成する。この力／温度入力メタデータベクトルを入力信号の統計モデルに変

換し、「良好な＿健康状態＿疲労している」（good_health_fatigued）というハンドルで基準として保存する。

【００６７】

後に、認識モードにおいて、ユーザーが無線装置１００を保持した際に、触覚センサ信号及び力センサ信号をサンプリングする。この健康／疲労状態の認識は、接触トランスデューサ信号のサンプリング及びデジタル化ステップによって構成される。次いで、これらのデジタル化されたセンサ信号を処理し、メタデータベクトルを生成する。そして、このメタデータベクトルを「良好な＿健康状態＿普通に＿休息している」及び「良好な＿健康状態＿疲労している」というハンドルを有する基準統計モデルと比較する。この結果、最もよくマッチしたものが接触認識の推定結果となる。

【００６８】

本発明による無線装置１００内の健康維持アプリケーションプログラムは、この認識結果を使用し、有用且つ適切な情報をユーザーに提供することができる。例えば、健康維持プログラムは、この認識結果を処理し、それに応答して、ユーザーに警告を発すると共に、感知された疲労を緩和するための薬剤について通知することができる。自動認識プログラムに伴う問題点の１つは、それらのプログラム自体が無線装置１００のメモリ容量と比べて大きかったり、それらのプログラムが呼び出すデータベースがメモリ容量と比べて大きかったりすることである。

【００６９】

本発明の別の態様においては、この認識結果を使用し、リモートサーバー内の補助的なアプリケーションプログラムが更なる詳細且つ有用で適切な情報をユーザーに提供可能である。例えば、このサーバーは、感知されたユーザーの疲労を緩和する薬剤情報に関する大きなデータベースにアクセスすることができる。そして、データベースの検索結果を無線装置１００に返すことができる。又、このサーバーは、ユーザーの特性と嗜好に関するパーソナルプロファイルを保持することもでき、データベースに対する問い合わせを自動生成する際に、このプロファイルを使用可能である。即ち、例えば、通知した薬剤によってユーザーにアレルギー反応が生じることのないように、ユーザーの薬剤アレルギー情報をサーバーのデータベースに保存することができるのである。

【００７０】

図２Ａは、無線装置１００、サーバー１４０、ウェブサーバー１６０の機能ブロックダイアグラムであり、これらの間でメタデータベクトル１３８及びプライバシー制御データ１５０’を交換する際のやり取りが示されている。これらの交換は、ＤＥＳ（Data Encryption Standard）などの対称セッションキーによってバルク暗号化されており、データのプライバシーが保護されている。メタデータベクトル１３８とプライバシー制御データ１５０’の完全性を保証するべく、前出のジョン・ワイリー・アンド・サンズ社（John Wiley and Sons）から２０００年に出版されたステファン・トーマス（Stephen Thomas）による「ＳＳＬとＴＬＳ（SSL and TLS）」という名称の書籍に記述されているように、ＭＡＣ（message authentication code）を算出し、データに添付することができる。メタデータベクトル１３８及びプライバシー制御データ１５０’のソースを保証するべく、前出のアディソン・ウェスリー社（Addison Wesley）から１９９７年に出版されたリチャードＥ．スミス（Richard E. Smith）による「インターネット暗号法（Internet Cryptography）」という名称の書籍に記述されているように、デジタル署名をデータに添付可能である。

【００７１】

図２Ａには、状況識別の実装を分散させたものが示されている。無線装置１００は、ダウンロードされるか或いはファームウェアの状態にある状況に応じたアプリケーションＡ、Ｂ、Ｘ、及びＹを備えている。この無線装置１００は、ネットワークサーバー１４０内の状況推定エンジン１４２（これは、データを処理し、生成された現在の状況を返送する能力を有している）に送信する前に、メタデータベクトル１３８内の状況情報の一部をローカルに事前処理することができる。又、無線装置１００は、状況に応じたサービスをモバイルユーザーに提供するためにウェブサービスサーバー１６０へのアクセスを必要とするアプリケーションプログラムを実行することも可能である。

【００７２】

図２Ａには、センサからのセンサデータの無線装置１００における処理を無線装置とネットワークサーバー１４０間で分散させる方法が示されている。この図２Ａの動作は、次のとおりである。

【００７３】

（１）センサがセンサデータを無線装置１００内の状況推定エンジン１３６に継続的に供給する。

【００７４】

（２）アプリケーションプログラムが状況識別ＡＰＩ１５４を利用して最新の状況情報を要求する（即ち、特定の状況情報の変化を受信するべく、アプリケーションプログラムを登録することができる）。

【００７５】

（３）状況推定エンジン１３６は、ネットワークサーバー１４０の状況推定エンジン１４２と安全にコンタクトし、メタデータベクトル１３８をサーバー１４０に送信する。センサ及び実装の詳細に応じて、状況推定エンジン１３６は、この送信の前に、メタデータベクトル１３８内のセンサデータの一部を事前処理することができる。又、センサと処理インターバルに応じて、状況推定エンジン１３６と状況推定エンジン１４２間に頻繁なデータ交換用の仮想的な接続を設けることも可能である。ネットワークサーバー１４０内の状況推定エンジン１４２は、メタデータベクトル１３８内の事前処理されたセンサデータの演算集約的及び／又はメモリ集約的な処理を実行して現在の状況に関する結果情報を生成するための処理能力とメモリ容量を備えている。

【００７６】

（４）ネットワークサーバー１４０内の状況推定エンジン１４２は、モバイルユーザーの現在の状況をより正確に判定するべく、ユーザーデータベース１４６内に保存されているローカルユーザー情報（履歴情報、顧客に関する詳細情報）を利用することができる。

【００７７】

（５）ネットワークサーバー１４０内の状況推定エンジン１４２は、無線装置１００内の状況推定エンジン１３６に現在の状況に関する識別情報を安全に返す。

【００７８】

（６）無線装置１００内の状況推定エンジン１３６は、情報を受信するべく登録されているアプリケーションプログラムに対し、この現在の状況に関する識別情報を状況識別ＡＰＩ１５４を介して提供する。

【００７９】

図２Ａには、ウェブサービスサーバー１６０内のウェブサービスが無線装置１００の現在の状況の推定結果を受信できるようにする方法が示されている。ウェブサービスサーバー１６０は、図２に示されている無線装置１００内のソフトウェアシステムＳＳＩ及び実行環境（Exec.Env.）に類似したサーバーアプリケーションプログラムＡ用のソフトウェアシステムとサーバーアプリケーションプログラムＸ及びＹ用の実行環境を備えている。これらのウェブサービスサーバー１６０内のサーバーアプリケーションプログラムＡ、Ｘ、及びＹは、無線装置１００の現在の状況をウェブサービスに提供するために状況識別ＡＰＩを介したアクセスを必要とすることがある。

【００８０】

図２Ａにおいて、ウェブサービスサーバー１６０は、状況推定クライアント１７６を使用してネットワークサーバー１４０内の状況推定サーバー１７４にコンタクトする。状況推定クライアント１７６は、データベース１８４内の顧客データベース情報を利用してウェブサーバー１６０の状況感知能力を向上させることができる。このネットワークサーバー１４０へのコンタクトは、ネットワークサーバー１４０内の状況推定サーバー１７４に対する状況識別インターフェイス１８６を介して実行される。

【００８１】

状況推定サーバー１７４は、ネットワークサーバー１４０のプライバシー制御１６４を介して、ウェブサーバー１６０のウェブサービスを状況推定エンジン１４２に登録する。プライバシー制御１６４は、無線装置１００のプライバシープロファイル１５２のキャッシュされた複写１４４を備えている。これにより、ネットワークサーバー１４０において、ウェブサーバー１６０からのアクセス要求に対するプライバシーチェック処理を実行することができる。ウェブサーバー１６０とネットワークサーバー１４０間の通信は、ＨＴＴＰＳやＳＳＬなどのインタ

ーネット保護プロトコルによって保護されている。状況推定サーバー１７４は、独自のサービスをウェブサービスとしてインターネット上のその他のウェブサーバーに公開可能であり、この場合に、ウェブサーバー１６０とネットワークサーバー１４０間のインターフェイス１８６は、ＳＯＡＰ（Simple Object Access Protocol）メッセージングプロトコルで搬送されるＸＭＬ（Extensible Markup Language）メッセージによって実装可能である。

【００８２】

ネットワークサーバー１４０内の状況推定エンジン１４２は、処理済のセンサメタデータベクトル１３８と、場合によっては、多少のアプリケーションＡＰＩ情報と、を無線装置１００の状況推定エンジン１３６から受信する。このネットワークサーバーの状況推定エンジン１４２は、ユーザーの行動と無線装置の過去の使用状況に関するユーザーデータベース１４６情報を備えている。又、このネットワークサーバーの状況推定エンジン１４２は、潜在的なユーザーに提供するべく、サードパーティのサービス（コンテンツ及び／又はサービスを提供するものなど）を備えることもできる。又、ユーザーに提供する内容をユーザープロファイル１４４によって変化させることも可能である。無線装置１００の状況推定エンジン１３６からネットワークの状況推定エンジン１４２に伝達される情報の特性は、無線装置１００のユーザーが管理するプライバシー制御１５０によって制御可能である。従って、ユーザーは、ネットワークの状況推定エンジン１４２を完全に又は部分的に無効にして、サードパーティのサービスが使用可能な彼／彼女の情報量を制御することができる。即ち、ユーザーは、プライバシー制御１５０により、彼／彼女のプライベート情報に対する第三者のアクセスを制御できるのである。

【００８３】

無線装置の状況推定エンジン１３６は、無線装置１００内に位置しているアプリケーションＡ、Ｂ、Ｘ、又はＹからＡＰＩインターフェイス１５４を介して入力を受信する。２５分後に会議が始まることを示すカレンダアプリケーションプログラムからの入力が、この一例である。更なる例としては、カレンダアプリケーションプログラムは、あなたが参加する予定のリサの誕生日が明日であることも通

ットベースのＧＰＲＳ及びＵＭＴＳは、低頻度の情報転送レートをサポート可能である。又、無線装置１００からネットワークの方向に実行されたその他のシグナリングに続いてネットワークの状況推定エンジン１４２用の情報を無線装置１００から添付として送信することにより、状況推定エンジン１３６の情報のネットワークサーバー１４０への別途の転送用の無線装置１００の無線送信機の別途の電源投入を省略することが有利である。

【００８５】

図１を再度参照すれば、ネットワークサーバー１４０、ＵＤＤＩ（Universal Description、Discovery and Integration）レジストリ１７０、及ぶ複数のウェブサイトサーバー１６０間の関係が示されている。ＵＤＤＩは、インターネットベースのレジストリの実質的な業界標準である。このＵＤＤＩレジストリ１７０により、ネットワークサーバー１４０は、インターネット上のサービス及びビジネス用の新規のウェブサイトを発見することができる。このようなサービス及びビジネスがＵＤＤＩレジストリ１７０によって識別された場合には、ネットワークサーバー１４０は、それら新規に発見されたウェブサイト上のアプリケーションプログラムによるユーザープライベートデータへの非認可のアクセスを防止するべく、図２Ａのモバイルユーザーのキャッシュされているプライバシープロファイル１４４を適用しなければならない。

【００８６】

図３は、無線装置１００の現在の状況を判定する際の無線装置１００（左の列）、ネットワークサーバー１４０（中央の列）、及びウェブサーバー１６０（右の列）間のやり取りを示すネットワークプロセスフローチャートである。このプロセスは、無線装置１００のステップ３０２から始まっている。

【００８７】

（ステップ３０２）無線装置１００内のプライバシー制御１５０は、更新済みのプライバシープロファイルをネットワークサーバー１４０に送信する。

【００８８】

次いで、ネットワークサーバー１４０がステップ３０４を実行する。

【００８９】

知してくれる。無線装置の状況推定エンジン１３６は、ネットワークサーバーの状況推定エンジン１４２に対し、処理済の結果情報を伝達することができる。この場合に、無線装置の状況推定エンジン１３６の意思決定においては、センサ情報に加えて、アプリケーションＡ、Ｂ、Ｘ、又はＹからの情報を使用することもできる。即ち、センサ情報とアプリケーションプログラムＡ、Ｂ、Ｘ、又はＹからの情報の組み合わせを状況推定エンジン１３６によって処理できるのである。アプリケーションプログラムの使用状況に関連し、ユーザーの行動又は使用パターンをセンサから検出してユーザーデータベースに記録することができる。前述のように、このセンサ及びアプリケーションプログラムからの情報の組み合わせの処理を状況推定エンジン１３６と状況推定エンジン１４２間で分担することができる。無線装置１００で稼動中のアプリケーションＡ、Ｂ、Ｘ、及びＹ、或いはウェブサーバー１６０において稼動中のサーバーアプリケーションプログラムＡ、Ｘ、及びＹは、任意選択により、ネットワークサーバー１４０内の状況推定エンジン１４２にもアプリケーションデータを提供することができる。状況推定エンジン１４２は、任意選択により、メタデータベクトル１３８及びアプリケーションデータを処理して現在の状況を生成可能である。

【００８４】

無線装置の状況推定エンジン１３６からネットワークサーバーの状況推定エンジン１４２への情報の転送は、複数の代替方法によって実行可能である。無線装置１００及びネットワークサーバー１４０間における現在の使用状況と転送容量を考慮し、システムを管理することができる。状況情報は、常に頻繁に収集する必要はない（例えば、数秒ごとに定期的にネットワーク側１４０に転送しなければならないというものではない）。アプリケーションに応じて、無線装置１００の状況推定エンジン１３６からサーバー１４０の状況推定エンジン１４２への情報転送に適用するタイミングウィンドウを秒単位のものから分単位のものに変化させることができる。無線装置１００の環境にイベントや状態の変化がない場合には、サーバー１４０の状況推定エンジン１４２に情報を転送する必要はない。又、情報を無線装置１００内のバッファ内に一時保存しておき、この情報を低頻度でネットワークの状況推定エンジン１４２に転送することも可能である。パケ

（ステップ３０４）ネットワークサーバー１４０は、キャッシュされているプライバシープロファイル１４４を更新する。

【００９０】

次いで、無線装置１００は、後続のステップ３０６、３０８、及び３１０を実行する。

【００９１】

（ステップ３０６）センサが、無線装置１００内の状況推定エンジン１３６に対してセンサデータを継続的に供給する。

【００９２】

（ステップ３０８）アプリケーションプログラムは、状況識別ＡＰＩ１５４を使用して最新の状況情報を要求する。

【００９３】

（ステップ３１０）状況推定エンジン１３６は、ネットワークサーバー１４０の状況推定エンジン１４２とコンタクトし、メタデータベクトル１３８をサーバー１４０に送信する。

【００９４】

次いで、ネットワークサーバー１４０は、ステップ３１２及び３１４を実行する。

【００９５】

（ステップ３１２）ネットワークサーバー１４０内の状況推定エンジン１４２は、ユーザーデータベース１４６内に保存されているローカルユーザー情報を使用し、モバイルユーザーの現在の状況をより正確に判定する。

【００９６】

（ステップ３１４）ネットワークサーバー１４０は、ウェブサーバー１６０に対してデータを要求する。

【００９７】

このネットワークサーバーのアクセスは、ネットワークサーバー内にキャッシュされているプライバシープロファイル１４４によって認可される。

【００９８】

次いで、ウェブサーバー１６０は、ステップ３１６を実行する。

【００９９】

（ステップ３１６）ウェブサーバーは、データベース１８４内に保存されているユーザー情報をネットワークサーバー１４０に提供する。

【０１００】

次いで、ネットワークサーバー１４０は、ステップ３１８を実行する。

【０１０１】

（ステップ３１８）ネットワークサーバー１４０内の状況推定エンジン１４２は、無線装置１００内の状況推定エンジン１３６に対して現在の状況認識情報を安全に返す。

【０１０２】

次いで、無線装置１００は、ステップ３２０において終了する。

【０１０３】

（ステップ３１８）無線装置１００内の状況推定エンジン１３６は、情報を受信するべく登録されているアプリケーションプログラムに対し、状況識別ＡＰＩ１５４を介して現在の状況識別情報を提供する。

【０１０４】

図４は、ネットワークサーバー１４０の機能ブロックダイアグラムであり、本発明の動作の実行に必要なアプリケーションサービスソフトウェアプログラムを保存するメモリ４０２が示されている。このメモリは、バス４０４により、キャッシュ１４４、ユーザーデータベース１４６、ＴＣＰ／ＩＰネットワークアダプタ４０６、及び中央プロセッサ４１０に接続されている。メモリ４０２は、プロセッサ４１０によって実行された際に本発明の方法を実行する実行形式命令のシーケンスであるプログラムを保存している。

【０１０５】

図４は、ネットワークサーバーの機能ブロックダイアグラムであり、本発明の実施例の動作の実行に必要なアプリケーションサービスソフトウェアプログラムを保存するメモリが示されている。図４には、オブジェクトモデルとして構成された模範的なネットワークサーバー１４０の機能コンポーネントが開示されてい

る。オブジェクトモデルとは、オブジェクト指向のソフトウェアプログラムをネットワークサーバー１４０内の主要機能及びアプリケーションを実行するコンポーネントにグループ化したものである。このネットワークサーバー１４０のメモリ４０２のオブジェクトモデルにおいては、プレゼンテーションティア４１５、インフラストラクチャオブジェクトパーティション４２２、及びビジネスロジックティア４１４からなる３つのティアアーキテクチャが採用されている。そして、このオブジェクトモデルでは、ビジネスロジックティア４１４が、アプリケーションオブジェクトパーティション４２２とデータオブジェクトパーティション４２６という２つのパーティションに更に分割されている。

【０１０６】

プレゼンテーションティア４１５は、ネットワークサーバー１４０に対する装置インターフェイスを管理するプログラムを保持している。図４においては、プレゼンテーションティア４１５は、ネットワークインターフェイス４２０を含んでいる。このプレゼンテーションティア４１５の好適な実装は、Ｊａｖａ（登録商標）サーブレットを使用し、ＨＴＴＰ（Hypertext Transfer Protocol）を介してＷＡＰプロトコルゲートウェイ１２０とやり取りするものである。これらのＪａｖａ（登録商標）サーブレットは、ＷＡＰプロトコルゲートウェイ１２０とネットワークサーバー１４０間におけるメッセージ交換を管理する要求／応答サーバー内で稼動する。Ｊａｖａ（登録商標）サーブレットとは、Ｗｅｂサーバー環境内で稼動するＪａｖａプログラムのことである。Ｊａｖａ（登録商標）サーブレットは、要求を入力として取得してそのデータを解析し、論理演算を実行した後に、応答をＷＡＰプロトコルゲートウェイ１２０に返す。Ｊａｖａ（登録商標）ランタイムプラットフォームは、複数のＪａｖａ（登録商標）サーブレットをプールしておき、多数の要求に対して同時にサービスする。ネットワークインターフェイス４２０は、ＷＡＰプロトコルゲートウェイ１２０から要求メッセージを受信し、更なる処理を実行するべく、要求内の情報をビジットオブジェクト４２８に渡す。ビジットオブジェクト４２８は、ＷＡＰプロトコルゲートウェイ１２０に返送するべく、処理結果をネットワークインターフェイス４２０に渡す。又、ネットワークインターフェイス４２０は、ネットワークアダプタ４０６

を使用して別のユーザー装置とデータ交換することも可能である。

【０１０７】

インフラストラクチャオブジェクトパーティション４２２は、ビジネスロジックティア４１４に代わって管理及びシステム機能を実行するプログラムを保持している。このインフラストラクチャオブジェクトパーティション４２２には、オペレーティングシステム４２５、データベースサーバーインターフェイス用のオブジェクト指向ソフトウェアプログラムコンポーネント４３０、及びシステム管理者インターフェイス４３２が含まれている。

【０１０８】

図４のビジネスロジックティア４１４には、ビジットオブジェクトの複数のインスタンス４２８、４２８’、４２８’’が含まれている。ビジットオブジェクト４２８の別個の各インスタンスは、それぞれのネットワークインターフェイス４２０のセッションごとに存在している。それぞれのビジットオブジェクト４２８は、１回のやり取りやメソッド呼び出しの際だけでなく、セッションの開始から終了に至るまで持続的な記憶領域を含むステートフルなセッションオブジェクトである。この持続的な記憶領域には、セッションに関連する情報が保持される。

【０１０９】

ＷＡＰプロトコルゲートウェイ１２０がメタデータベクトル１３８メッセージをネットワークサーバー１４０に送信すると、このメッセージは、ネットワークインターフェイス４２０に送信され、ビジットオブジェクト４２８を作成し接続情報を状態としてビジットオブジェクト４２８に保存するメソッドが呼び出される。そして、ビジットオブジェクト４２８は、状況推定エンジン１４２のアプリケーション４４０内のメソッドを呼び出してメタデータベクトルに基づいて状況推定を実行し、現在の状況に関する結果を返すことができる。

【０１１０】

ＷＡＰプロトコルゲートウェイ１２０がプライバシー制御データ１５０’メッセージをネットワークサーバー１４０に送信すると、このメッセージは、ネットワークインターフェイス４２０に送信され、ビジットオブジェクト４２８を生成し接続情報を状態としてビジットオブジェクト４２８に保存するメソッドが呼び出される。そして、ビジットオブジェクト４２８は、プライバシー制御１６４のアプリケーション４４２内のメソッドを呼び出し、キャッシュされているプライバシープロファイル１４４を更新することができる。アプリケーション４４２は、プライバシープロファイル更新アプリケーション４４８に対してメソッド呼び出しを実行し、更新済みのデータ１５０’をキャッシュ１４４内に保存する。

【０１１１】

ＷＡＰプロトコルゲートウェイ１２０がユーザーデータ更新メッセージをネットワークサーバー１４０に送信すると、このメッセージは、ネットワークインターフェイス４２０に送信され、ビジットオブジェクト４２８を生成し接続情報を状態としてビジットオブジェクト４２８に保存するメソッドが呼び出される。そして、ビジットオブジェクト４２８は、ユーザーデータベースアプリケーション４４６内のメソッドを呼び出し、ユーザーデータをデータベース１４６内に保存することができる。

【０１１２】

Enterprise Java Beansによって開発されたサーバープログラミングアプリケーションについては、１９９９年にジョン・ワイリー・アンド・サンズ社（John Wiley and Sons）から出版されたエド・ロマン（Ed Roman）による「Enterprise Java Beansの習得（Mastering Enterprise Java Beans）」という名称の書籍に記述されている。サーバーアプリケーションの設計におけるオブジェクトモデルの使用法については、２０００年にロックス・プレス社（Wrox Press Inc.）から出版されたマシュー・レイノルズ（Matthew Reynolds）による「Ｅコマースを始める（Beginning E-Commerce）」という名称の書籍（ISBN:1861003986）に記述されている。Ｊａｖａ（登録商標）サーブレットとウェブサイトサーバーの開発については、２０００年にマニング・パブリケーションズ社（Manning Publications Co.）から出版されたデュアンＫ．フィールズ（Duane K. Fields）他による「Ｊａｖａ（登録商標）サーバー頁によるウェブ開発（Web Developments with Java Server Pages）」という書籍に記述されている。

【０１１３】

状況に応じたウェブサービスに関する本発明により、携帯電話又は無線装置１０

０は、状況推定技法を使用してユーザーの環境を感知し、これに応答し、感知されたユーザー環境に適した有用な情報をユーザーに提供することができる。そして、モバイルユーザーには、ネットワーク内に存在するアプリケーションプログラムによるユーザープライベートデータへのアクセスを制御する機能が提供される。

以上、本発明の特定の実施例について開示したが、当業者であれば、本発明の精神と範囲を逸脱することなく、これらの特定の実施例に変更を加えることが可能であることを理解するであろう。

【図面の簡単な説明】

【０１１４】

【図１】本発明のネットワーク図であり、ユーザーのＷＡＰ（Wireless Application Protocol）に対応した携帯型無線装置、インターネットに対するＷＡＰプロトコルゲートウェイ、ネットワークサーバー、ＵＤＤＩ（Universal Description, Discovery and Integration）レジストリ、及び複数のウェブサイト間の関係の一例を示している。

【図１Ａ】「状況に応じたサービス」メニューのサブメニューである「プライバシー機能の更新」を有するユーザーの無線装置を示しており、ユーザーは、このサブメニューにより、「あなたのプライバシープロファイルの更新」と「あなたの個人情報の更新」を実行することができる。

【図１Ｂ】「状況に応じたサービス」メニューのサブメニューである「プライバシー機能の更新」を有するユーザーの無線装置を示しており、ユーザーは、このサブメニューにより、「プログラムの認証」と「プログラムの登録」を実行することができる。

【図１Ｃ－１Ｄ】「状況に応じたサービス」メニューのサブメニューである「アプリケーションの実行」を有するユーザーの無線装置を示しており、ユーザーは、このサブメニューにより、「アプリケーションの実行」を行うことができる。

【図２】無線装置１００の機能ブロックダイアグラムであり、その様々なコンポーネントとプログラムが示されている。

【図２Ａ】無線装置１００、サーバー１４０、及びウェブサーバー１６０の機能ブロックダイアグラムであり、メタデータベクトル１３８及びプライバシー制御データ１５０を交換する際のそれらの間のやり取りが示されている。

【図３】無線装置１００の現在の状況に関する判定を実行する際の無線装置１００、ネットワークサーバー１４０、及びウェブサーバー１６０間のやり取りを示すネットワークプロセスフローチャートである。

【図４】ネットワークサーバー１４０の機能ブロックダイアグラムであり、本発明の動作を実行するのに必要なアプリケーションサービスソフトウェアプログラムを保存するメモリを示している。

【図１】

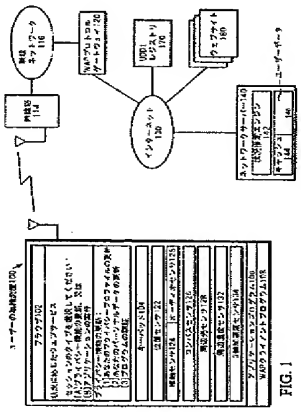


FIG. 1

【図１Ａ】

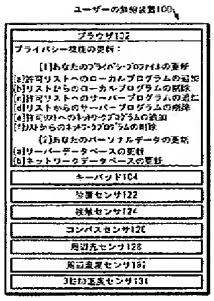


FIG. 1A

【図１Ｂ】

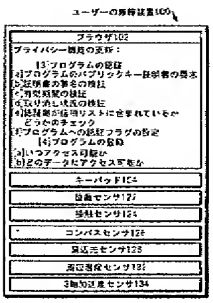


FIG. 1B

【図１Ｃ】

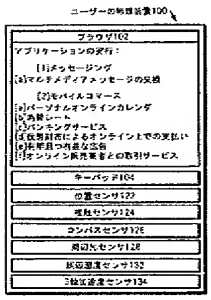


FIG. 1C

【図１Ｄ】

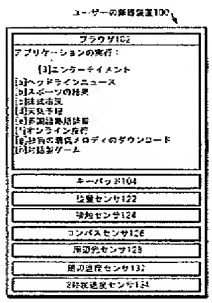
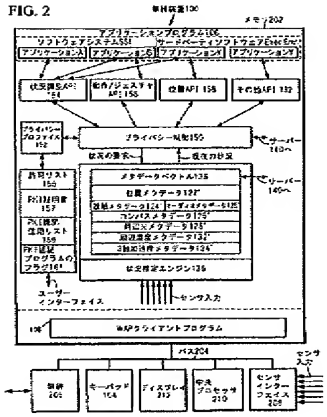


FIG. 1D

【図２】

FIG. 2



【図２Ａ】

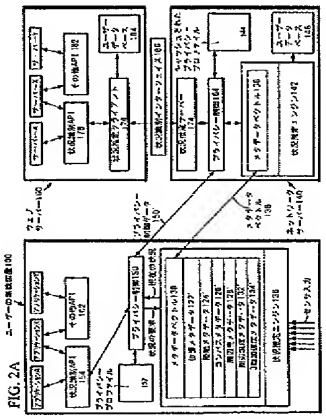


FIG. 2A

【図３】

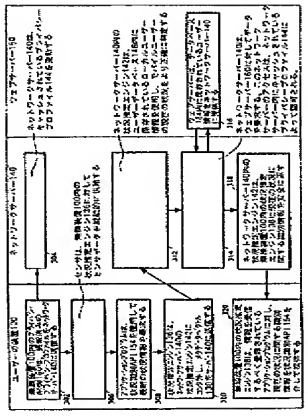
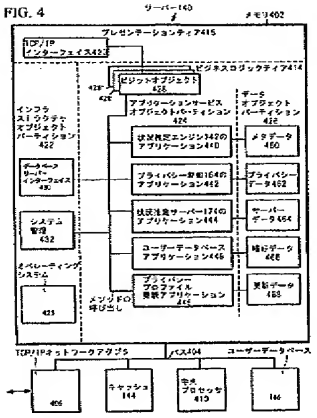


FIG. 3

【図４】

FIG. 4



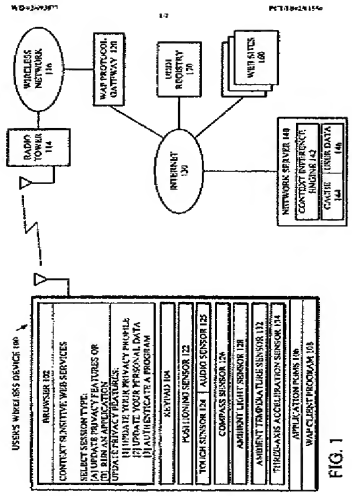


FIG. 1

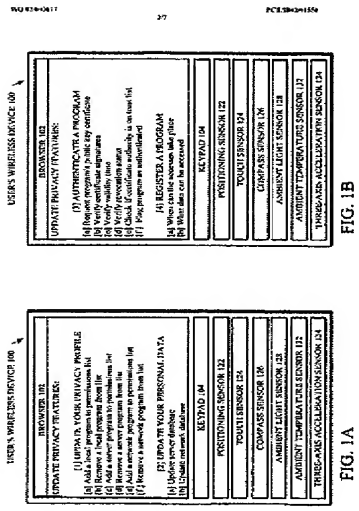


FIG. 1B

FIG. 1A

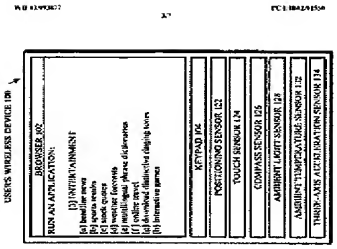


FIG. 1D

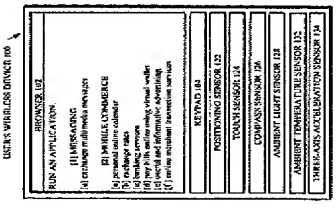
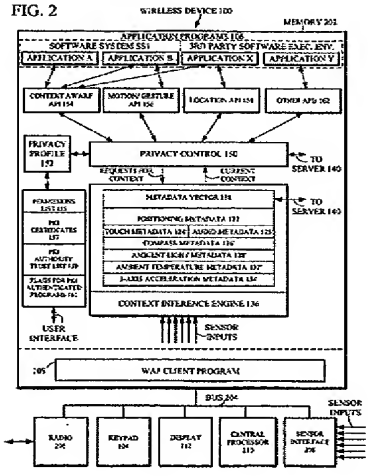


FIG. 1C

FIG. 2



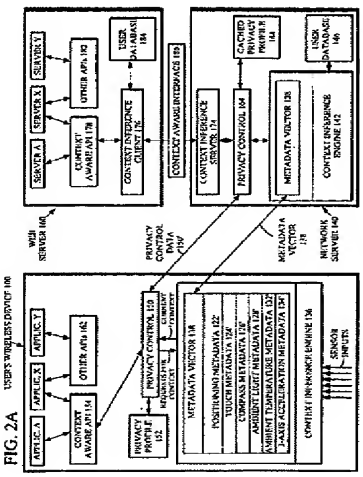


FIG. 2A

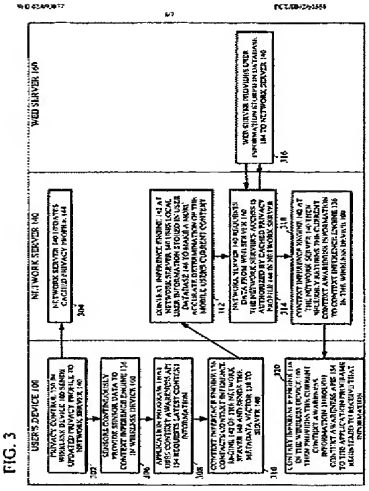


FIG. 3

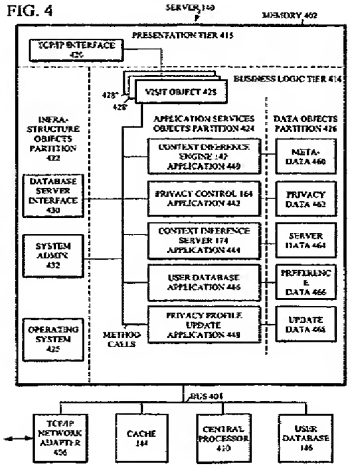


FIG. 4

フロントページの続き

(81)指定国　AP(GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW

(72)発明者　ニュカネン，ペトリ
フィンランド国，エフイーエンー３７１２０　ノキア，レードッキカトゥ　３
(72)発明者　パロニエミ，ヤリ
フィンランド国，エフイーエンー９０９００　キーミンキ，イリキーミンギンティエ　１６９
(72)発明者　カンガス，ペトリ
フィンランド国，エフイーエンー９０８００　オウル，ポルッキティエ　７アー３

Ｆターム(参考)　5B085 AA08
5K067 AA34 BB04 BB21 DD20 DD27 DD30 DD51 EE02 EE10 EE16
HH21 JJ52
5K101 KK16 LL12 MM07 NN01 NN18

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB02/01558

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : H04B 1/00, 3/00, 3/42, 11/10; H03B 1/58
US Cl. : 455/3.03, 402, 405, 412-420, 456, 458, 466, 515, 550, 556, 575
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
U.S. : 455/3.03, 402, 405, 412-420, 456, 458, 466, 515, 550, 556, 575

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
NONE

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 6,115,611 A (KIMOTO et al) 05 September 2000, figs. 1, 7-8, 10, 12, 19, 27, 31, 42.	1-38 --- 39-41
Y	US 6,073,075 A (KONDOU et al) 06 June 2000, fig. 3, column 4 lines 26-42.	39-41

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 July 2002 (19.07.2002)	27 AUG 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer William Trost Telephone No. 703 306-0377

Form PCT/ISA/210 (second sheet) (July 1998)

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成17年7月28日(2005.7.28)

【公表番号】特表2004-535000(P2004-535000A)
【公表日】平成16年11月18日(2004.11.18)
【年通号数】公開・登録公報2004-045
【出願番号】特願2002-590624(P2002-590624)
【国際特許分類第７版】
Ｇ０６Ｆ　15/00
Ｈ０４Ｍ　11/00
Ｈ０４Ｑ　 7/20
【ＦＩ】
Ｇ０６Ｆ　15/00　３１０Ａ
Ｈ０４Ｍ　11/00　３０２
Ｈ０４Ｑ　 7/04　Ｚ

【手続補正書】
【提出日】平成15年12月5日(2003.12.5)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
無線装置が、該装置の現在の環境に関連する情報をそのユーザーに提供する方法であって、
前記信号は第１環境信号と第２環境信号を含む、前記無線装置の現在の環境を特徴付けるセンサ信号を受信するステップと、
前記第１環境信号と前記第２環境信号を合成センサ信号に合成するステップと
前記合成センサ信号を前記無線装置内の状況推定エンジンによって処理するステップと、
前記状況推定エンジンによる処理によって生成された現在の状況に関する結果を出力するステップと、
前記現在の状況に関する結果に応答し、前記ユーザーに情報を提供するステップと、
を有する方法。
【請求項２】
前記状況推定エンジンによるセンサ信号の処理は、前記ユーザーの無線装置内で稼動するプログラムされた命令として実施される請求項１記載の方法。
【請求項３】
前記ユーザーの無線装置からの信号に応答し、別個のネットワークサーバー内で実行される、プログラムされた命令を実装した第２の状況推定エンジンにより、センサ信号を処理するステップを更に含む、請求項１記載の方法。
【請求項４】
前記サーバーは、前記ユーザーの無線装置に対して選択的に転送すべく、ウェブサーバーのファイルにアクセスする請求項３記載の方法。
【請求項５】
前記無線装置は、前記センサ信号の処理の一部を前記サーバー内の第２の状況推定エンジンに、負荷分散する請求項３記載の方法。

【請求項６】
前記ユーザーのパーソナルプロファイルを、前記サーバーが保持する請求項３記載の方法。
【請求項７】
アプリケーションプログラムによる前記ユーザープライベートデータに対するアクセスのユーザー制御を提供するステップを、
更に有する請求項１記載の方法。
【請求項８】
アプリケーションプログラムによる前記サーバー内の前記ユーザープライベートデータに対するアクセスのユーザー制御を提供するステップ、
を更に有する請求項３記載の方法。
【請求項９】
ウェブサーバー内のアプリケーションプログラムによる前記ユーザープライベートデータに対するアクセスのユーザー制御を提供するステップ、
を更に有する請求項１記載の方法。
【請求項１０】
前記現在の状況に関する結果をアプリケーションプログラムに提供するステップと、
前記アプリケーションプログラムから前記ユーザーに対する有用な情報を受信するステップと、
を更に有する請求項１記載の方法。
【請求項１１】
アプリケーションプログラムによる前記現在の状況に関する結果に対するアクセスのユーザー制御を提供するステップと、
前記ユーザー制御に応答し、前記現在の状況に関する結果を前記アプリケーションプログラムに提供するステップと、
前記アプリケーションプログラムから前記有用な情報を受信するステップと、
を更に有する請求項１記載の方法。
【請求項１２】
プライバシープロファイル内に保存された前記ユーザーのデータに基づいて、前記現在の状況に関する結果にアクセスするためのアクセス許可を前記アプリケーションプログラムに対して付与するステップを、
更に有する請求項１１記載の方法。
【請求項１３】
前記アクセスのユーザー制御を提供するステップが、前記ユーザーの無線装置からの信号に応答し、別個のネットワークサーバー内で実行されるプログラムされた命令として実施される請求項１１記載の方法。
【請求項１４】
前記プライベートなユーザーの現在の状況に関する結果に対するユーザー制御を提供しつつ、前記無線装置内の状況に応じたアプリケーション及びサービスを実現するステップを、
更に有する請求項１記載の方法。
【請求項１５】
前記プライベートなユーザーの現在の状況に関する結果に対するユーザー制御を提供しつつ、前記ネットワークサーバー内の状況に応じたアプリケーション及びサービスを実現するステップを、
更に有する請求項１記載の方法。
【請求項１６】
無線装置が、該装置の現在の環境に関連した情報をそのユーザーに対して提供できるようにする装置であって、
プロセッサと；

前記プロセッサに接続されたメモリであって、
第１環境信号と第２環境信号を含む前記無線装置の現在の環境を特徴付けるセンサ信号を受信するステップと、
前記第１環境信号と前記第２環境信号を合成センサ信号に合成するステップと
前記合成センサ信号を、前記無線装置内の状況推定エンジンによって処理するステップと、
前記状況推定エンジンによる処理によって生成された現在の状況に関する結果を出力するステップと、
前記現在の状況に関する結果に応答し、前記ユーザーに情報を提供するステップと、
を実行するべくプログラムされたメモリと；
を有する装置。
【請求項１７】
前記ユーザーの無線装置からの信号に応答して、前記センサー信号を処理する別個のネットワークサーバー内に第２状況推定エンジン、
を更に含む請求項１６記載の装置。
【請求項１８】
無線装置の現在の環境に関連した情報をそのユーザーに提供する前記無線装置であって、
前記無線装置の現在の環境を特徴付ける、第１環境信号と第２環境信号を供給する第１環境センサと第２環境センサーと、
第１環境信号と第２環境信号を合成センサー信号として合成するロジックと、
前記センサに接続され、前記合成センサ信号を処理し、前記処理によって生成された現在の状況に関する結果を提供する、前記無線装置における状況推定エンジンと、
前記状況推定エンジンに接続され、前記現在の状況に関する結果に応答し、情報を前記ユーザーに提供する出力装置と、
を有する無線装置。
【請求項１９】
無線装置の現在の環境に関連する情報をそのユーザーに提供する前記無線装置であって、
アプリケーションプログラムによる前記ユーザーのプライベートデータに対するアクセスのユーザー制御を提供するプライバシー制御と、
前記無線装置の現在の環境を特徴付けるセンサ信号を供給するセンサと、
前記センサに接続され、前記センサ信号を処理する前記無線装置における状況推定エンジンであって、前記プライバシー制御にも接続されており、前記処理によって生成された現在の状況に関する結果を前記アプリケーションプログラムに提供する状況推定エンジンと、
前記プライバシー制御に接続され、前記アプリケーションプログラムに応答し、情報を前記ユーザーに提供する出力装置と、
を有する無線装置。
【請求項２０】
無線装置の現在の環境に関連する情報を前記無線装置のユーザーに提供するシステムであって、
前記無線装置からユーザープライバシープロファイルを受信し、アプリケーションプログラムによる前記ユーザーのプライベートデータに対するアクセスセキュリティのユーザー制御を提供するサーバー内のプライバシー制御と、
前記無線装置の現在の環境を特徴付けるセンサ信号を供給する前記無線装置内のセンサと、
前記無線装置に接続され、前記センサ信号から導出されたセンサ情報を処理する前記サーバー内の状況推定エンジンであって、前記プライバシー制御に接続されており、前記処理によって生成された現在の状況に関する結果を前記アプリケーションプログラムに提供

する状況推定エンジンと、
前記プライバシー制御に接続され、前記アプリケーションプログラムに応答し、情報を前記無線装置に送信する出力装置と、
を有するシステム。

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成17年12月22日(2005.12.22)

【公表番号】特表2004-535000(P2004-535000A)
【公表日】平成16年11月18日(2004.11.18)
【年通号数】公開・登録公報2004-045
【出願番号】特願2002-590624(P2002-590624)
【国際特許分類第７版】
Ｇ０６Ｆ　15/00
Ｈ０４Ｍ　11/00
Ｈ０４Ｑ　 7/20
【ＦＩ】
Ｇ０６Ｆ　15/00　３１０Ａ
Ｈ０４Ｍ　11/00　３０２
Ｈ０４Ｑ　 7/04　Ｚ

【手続補正書】
【提出日】平成17年3月18日(2005.3.18)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
無線装置が、該装置の現在の環境に関連する情報をそのユーザーに提供する方法であって、
第１環境信号と第２環境信号を含む、前記無線装置の現在の環境を特徴付けるセンサ信号を受信するステップと、
前記第１環境信号と前記第２環境信号を合成しコンポジットセンサ信号にするステップと
前記コンポジットセンサ信号を前記無線装置内の状況推定エンジンによって処理するステップと、
前記状況推定エンジンによる処理によって生成された現在の状況に関する結果を出力するステップと、
前記現在の状況に関する結果に応答し、前記ユーザーに情報を提供するステップと、
を有する方法。
【請求項２】
前記状況推定エンジンによるセンサ信号の処理は、前記ユーザーの無線装置内で稼動するプログラムされた命令として実施される請求項１記載の方法。
【請求項３】
前記ユーザーの無線装置からの信号に応答し、別個のネットワークサーバー内で実行される、プログラムされた命令を実装した第２の状況推定エンジンにより、センサ信号を処理するステップを更に含む、請求項１記載の方法。
【請求項４】
前記サーバーは、前記ユーザーの無線装置に対して選択的に転送すべく、ウェブサーバーのファイルにアクセスする請求項３記載の方法。
【請求項５】
前記無線装置が、前記センサ信号の処理の一部を前記サーバー内の第２の状況推定エン

ジンに、負荷分散する請求項３記載の方法。
【請求項６】
前記ユーザーのパーソナルプロファイルを、前記サーバーが保持する請求項３記載の方法。
【請求項７】
アプリケーションプログラムによる前記ユーザープライベートデータに対するアクセスのユーザー制御を提供するステップを、
更に有する請求項１記載の方法。
【請求項８】
アプリケーションプログラムによる前記サーバー内の前記ユーザープライベートデータに対するアクセスのユーザー制御を提供するステップ、
を更に有する請求項３記載の方法。
【請求項９】
ウェブサーバー内のアプリケーションプログラムによる前記ユーザープライベートデータに対するアクセスのユーザー制御を提供するステップ、
を更に有する請求項１記載の方法。
【請求項１０】
前記現在の状況に関する結果をアプリケーションプログラムに提供するステップと、
前記アプリケーションプログラムから前記ユーザーのための情報を受信するステップと、
を更に有する請求項１記載の方法。
【請求項１１】
アプリケーションプログラムによる前記現在の状況に関する結果に対するアクセスのユーザー制御を提供するステップと、
前記ユーザー制御に応答し、前記現在の状況に関する結果を前記アプリケーションプログラムに提供するステップと、
前記アプリケーションプログラムから前記情報を受信するステップと、
を更に有する請求項１記載の方法。
【請求項１２】
プライバシープロファイル内に保存された前記ユーザーのデータに基づいて、前記現在の状況に関する結果にアクセスするためのアクセス許可を前記アプリケーションプログラムに対して付与するステップを、
更に有する請求項１１記載の方法。
【請求項１３】
前記アクセスのユーザー制御を提供するステップが、前記ユーザーの無線装置からの信号に応答し、別個のネットワークサーバー内で実行されるプログラムされた命令として実施される請求項１１記載の方法。
【請求項１４】
前記サーバーは、前記ユーザーの無線装置に対して選択的に転送するべく、ウェブサーバーのファイルにアクセスする請求項１３記載の方法。
【請求項１５】
前記無線装置は、前記アクセスのユーザー制御を提供するステップの処理の一部を、前記サーバーに負荷分散する請求項１３記載の方法。
【請求項１６】
前記ユーザーのパーソナルプロファイルを前記サーバーが保持する請求項１３記載の方法。
【請求項１７】
アプリケーションプログラムによる前記ユーザーパーソナルプロファイルに対するアクセスのユーザー制御を提供するステップを、更に有する請求項１６記載の方法。
【請求項１８】

アプリケーションプログラムによる前記サーバー内の前記ユーザーパーソナルプロファイルに対するアクセスのユーザー制御を提供するステップを、更に有する請求項１３記載の方法。

【請求項１９】

ウェブサーバー内のアプリケーションプログラムによる前記ユーザープライベートデータに対するアクセスのユーザー制御を提供するステップを、更に有する請求項１１記載の方法。

【請求項２０】

前記プライベートなユーザーの現在の状況に関する結果に対するユーザー制御を提供しつつ、前記無線装置内の状況に応じたアプリケーション及びサービスを実現するステップを、
更に有する請求項１９記載の方法。

【請求項２１】

前記プライベートなユーザーの現在の状況に関する結果に対するユーザー制御を提供しつつ、前記ネットワークサーバー内の状況に応じたアプリケーション及びサービスを実現するステップを、
更に有する請求項１９記載の方法。

【請求項２２】

無線装置が、該装置の現在の環境に関連した情報をそのユーザーに対して提供できるようにする装置であって、

プロセッサと、

前記プロセッサに接続されたメモリであって、

第１環境信号と第２環境信号を含む前記無線装置の現在の環境を特徴付けるセンサ信号を受信するステップと、

前記第１環境信号と前記第２環境信号を合成しコンポジットセンサ信号にするステップと、

前記コンポジットセンサ信号を、前記無線装置内の状況推定エンジンによって処理するステップと、

前記状況推定エンジンによる処理によって生成された現在の状況に関する結果を出力するステップと、

前記現在の状況に関する結果に応答し、前記ユーザーに情報を提供するステップと、

を実行するべくプログラムされたメモリと；

を有する装置。

【請求項２３】

前記状況推定エンジンによるセンサ信号の処理は、前記ユーザーの無線装置内で稼動するプログラムされた命令として実装される請求項２２記載の装置。

【請求項２４】

前記ユーザーの無線装置からの信号に応答して、前記センサー信号を処理する別個のネットワークサーバー内に第２状況推定エンジン、
を更に含む請求項２２記載の装置。

【請求項２５】

前記サーバーは、前記ユーザーの無線装置に対して選択的に転送するべく、ウェブサーバーのファイルにアクセスする請求項２４記載の装置。

【請求項２６】

無線装置の現在の環境に関連した情報をそのユーザーに提供する前記無線装置であって、

前記無線装置の現在の環境を特徴付ける、第１環境信号と第２環境信号を供給する第１環境センサと第２環境センサーと、
第１環境信号と第２環境信号を合成しコンポジットセンサ信号とするロジックと、

前記センサに接続され、前記コンポジットセンサ信号を処理し、前記処理によって生成

された現在の状況に関する結果を提供する、前記無線装置における状況推定エンジンと、
前記状況推定エンジンに接続され、前記現在の状況に関する結果に応答し、情報を前記ユーザーに提供する出力装置と、
を有する無線装置。
【請求項２７】
無線装置の現在の環境に関連する情報をそのユーザーに提供する前記無線装置であって、
アプリケーションプログラムによる前記ユーザーのプライベートデータに対するアクセスのユーザー制御を提供するプライバシー制御と、
前記無線装置の現在の環境を特徴付けるセンサ信号を供給するセンサと、
前記センサに接続され、前記センサ信号を処理する前記無線装置における状況推定エンジンであって、前記プライバシー制御にも接続されており、前記処理によって生成された現在の状況に関する結果を前記アプリケーションプログラムに提供する状況推定エンジンと、
前記プライバシー制御に接続され、前記アプリケーションプログラムに応答し、情報を前記ユーザーに提供する出力装置と、
を有する無線装置。
【請求項２８】
無線装置の現在の環境に関連する情報を前記無線装置のユーザーに提供するシステムであって、
前記無線装置からユーザープライバシープロファイルを受信し、アプリケーションプログラムによる前記ユーザーのプライベートデータに対するアクセスセキュリティのユーザー制御を提供するサーバー内のプライバシー制御と、
前記無線装置の現在の環境を特徴付けるセンサ信号を供給する前記無線装置内のセンサと、
前記無線装置に接続され、前記センサ信号から導出されたセンサ情報を処理する前記サーバー内の状況推定エンジンであって、前記プライバシー制御に接続されており、前記処理によって生成された現在の状況に関する結果を前記アプリケーションプログラムに提供する状況推定エンジンと、
前記プライバシー制御に接続され、前記アプリケーションプログラムに応答し、情報を前記無線装置に送信する出力装置と、
を有するシステム。
【請求項２９】
無線装置が、該装置の現在の環境に関係した情報をそのユーザーに提供できるようにする方法であって、
アプリケーションデータを前記無線装置に供給するプログラムを実行するステップと、
前記無線装置の現在の環境を特徴付ける、第１環境信号と第２環境信号を有するセンサ信号を受信するステップと、
前記第１環境信号と第２環境信号を合成しコンポジットセンサ信号にするステップと、
前記コンポジットセンサ信号と前記アプリケーションデータを状況推定エンジンによって処理するステップと、
前記状況推定エンジンによる処理によって生成された現在の状況に関する結果を出力するステップと、
前記現在の状況に関する結果に応答し、前記ユーザーに情報を提供するステップと、
を有する方法。
【請求項３０】
前記状況推定エンジンによるセンサ信号の処理は、前記ユーザーの無線装置内で稼動するプログラムされた命令として実装される請求項２９記載の方法。
【請求項３１】
前記プログラムを実行するステップは、前記無線装置において実行される請求項３０記

載の方法。
【請求項３２】
請求項２９記載の方法であって、ユーザーの無線装置からの信号に応答して、別のネットワークサーバ内で稼動するプログラムされた命令として実装される第２状況推定エンジンを使って、前記コンポジットセンサ信号を処理するステップを、
更に有する請求項２９記載の方法。
【請求項３３】
プログラムを実行するステップは、前記ネットワークサーバーに接続されたウェブサーバーにおいて実行される請求項３２記載の方法。
【請求項３４】
無線装置が、該装置の現在の環境に関係した情報をそのユーザーに提供できるようにするシステムであって、
プロセッサと、
前記プロセッサに接続されたメモリであって、
アプリケーションデータを前記無線装置に供給するプログラムを実行するステップと、
前記無線装置の現在の環境を特徴付ける、第１環境信号と第２環境信号を有するセンサ信号を受信するステップと、
前記第１環境信号と第２環境信号を合成しコンポジットセンサ信号にするステップと、
前記コンポジットセンサ信号と前記アプリケーションデータを状況推定エンジンによって処理するステップと、
前記状況推定エンジンによる処理によって生成された現在の状況に関する結果を出力するステップと、
前記現在の状況に関する結果に応答し、前記ユーザーに情報を提供するステップと、
を実行するべくプログラムされたメモリと、
を有するシステム。
【請求項３５】
前記状況推定エンジンによる前記センサ信号と前記アプリケーションデータの処理が、前記ユーザーの無線装置内で稼動するプログラムされた命令として実装される請求項３４記載のシステム。
【請求項３６】
前記プログラムを実行するステップは、前記無線装置において実行される請求項３５記載のシステム。
【請求項３７】
前記ユーザーの無線装置からの信号に応答し前記センサ信号と前記アプリケーションデータを処理すべく、前記状況推定エンジンが、別個のネットワークサーバー内で稼動するプログラムされた命令として実装される請求項３４記載のシステム。
【請求項３８】
前記プログラムを実行するステップは、前記ネットワークサーバーに接続されたウェブサーバーにおいて実行される請求項３７記載のシステム。
【請求項３９】
無線装置が、該装置の現在の環境に関係する情報をそのユーザーに提供できるようにする方法であって、
第１環境信号と第２環境信号を有する、前記無線装置の現在の環境を特徴付けるセンサ信号を受信するステップと、
前記第１環境信号と第２環境信号を合成しコンポジットセンサ信号にするステップと、
前記ユーザーの無線装置内の第１状況推定エンジンによって、前記センサ信号を部分的に処理するステップと、
前記部分的に処理されたセンサ信号を、別個のネットワークサーバー内の第２状況推定エンジンに送信するステップと、
前記第２状況推定エンジンによって前記信号の処理を完了させるステップと、

前記第２状況推定エンジンによって生成された現在の状況に関する結果を、前記無線装置に送信するステップと、
前記現在の状況に関する結果に応答し、前記ユーザーに情報を提供するステップと、
を有する方法。
【請求項４０】
無線装置が、該装置の現在の環境に関係した情報をそのユーザーに提供できるようにするシステムであって、
第１環境信号と第２環境信号を有する、前記無線装置の現在の環境を特徴付けるセンサ信号を受信する無線装置と、
前記第１環境信号と第２環境信号を合成しコンポジットセンサ信号にするためのロジックと、
前記センサ信号を部分的に処理する前記ユーザーの無線装置内の第１状況推定エンジンと、
前記無線装置から送信された前記部分的に処理されたセンサ信号を受信し、前記センサ信号の処理を完了させる別個のネットワークサーバー内の第２状況推定エンジンと、
を有し、
前記第２状況推定エンジンは、現在の状況に関する結果を前記第２推定エンジンから前記無線装置に送信し、
前記無線装置は、前記現在の状況に関する結果に応答し、情報を前記ユーザーに提供することを特徴とするシステム。
【請求項４１】
無線装置が、該装置の現在の環境に関連する情報をそのユーザーに提供できるようにする方法であって、
第１環境信号と第２環境信号を有する、前記無線装置の現在の環境を特徴付けるセンサ信号を受信するステップと、
前記第１環境信号と第２環境信号を合成しコンポジットセンサ信号にするためのステップと、
前記ユーザーの無線装置内の第１状況推定エンジンによって前記コンポジットセンサ信号を部分的に処理するステップと、
前記部分的に処理されたセンサ信号を、別個のネットワークサーバー内の第２状況推定エンジンに送信するステップと、
前記第２状況推定エンジンによって前記センサ信号の処理を完了させるステップと、
現在の状況に関する結果を前記ネットワークサーバーから第２サーバーに転送するステップと、
前記現在の状況に関する結果に応答し、前記第２サーバーから前記ユーザーの無線装置に情報を送信するステップと、
を有する方法。
【請求項４２】
無線装置が、該装置の現在の環境に関連する情報をそのユーザーに提供できるようにする方法であって、
第１環境信号と第２環境信号を有する、前記無線装置の現在の環境を特徴付けるセンサ信号を受信するステップと、
前記第１環境信号と第２環境信号を合成しコンポジットセンサ信号にするためのステップと、
前記ユーザーの無線装置内の状況推定エンジンによって前記コンポジットセンサ信号を処理するステップと、
前記状況推定エンジンによる処理によって生成された現在の状況に関する結果を、出力するステップと、
現在の状況に関する結果に応答しアプリケーションプログラムによるアクセスのユーザコントロールを提供するステップと、

ユーザコントロールに応答してアプリケーションプログラムに、現在の状況に関する結果を提供するステップと、
現在の状況に関する結果に応答して、アプリケーションプログラムから情報を受信するステップと、
を有する方法。
【請求項４３】
無線装置が、該装置の現在の環境に関係た情報をそのユーザーに提供できるようにする方法であって、
第１環境信号と第２環境信号を有する、前記無線装置の現在の環境を特徴付けるセンサ信号を受信するステップと、
前記第１環境信号と第２環境信号を合成しコンポジットセンサ信号にするステップと、
ユーザーの無線装置からの信号に応答して、別のネットワークサーバ内で稼動するプログラムされた命令として実装される状況推定エンジンにより前記コンポジットセンサ信号を処理するステップと、
前記状況推定エンジンにより処理された現在の状況に関する結果を出力するステップと、
アプリケーションプログラムによるアクセスのユーザコントロールを現在の状況に関する結果に提供するステップであって、前記ユーザコントロールは、ユーザーの無線装置からの信号に応答して別のネットワークサーバ内で稼動するプログラムされた命令として実装されることを特徴とするステップと、
ユーザコントロールに応答して、アプリケーションプログラムに現在の状況に関する結果を提供するステップと、
アプリケーションプログラムから情報を受信するステップと、
を有する方法。
【請求項４４】
ユーザのパーソナルプロファイルは、サーバにより保持されることを特徴とする請求項４３記載の方法。
【請求項４５】
ユーザのパーソナルプロファイルに対し、アプリケーションプログラムによるアクセスのユーザコントロールを提供するステップを、更に有する請求項４４記載の方法。
【請求項４６】
ユーザーの現在の状況のプライバシーに関しユーザー制御を提供しつつ、前記ネットワークサーバ内において状況に敏感なアプリケーション（context sensitive application）及びサービスを実現するステップを、
更に有する請求項４５記載の方法。
【請求項４７】
無線装置が、該装置の現在の環境に関連した情報をそのユーザーに対して提供できるようにするコンピュータプログラムプロダクトであって、
コンピュータ読み出し可能な媒体と，
第１環境信号と第２環境信号を含む、前記無線装置の現在の環境を特徴付けるセンサ信号を受信するための、前記コンピュータ読み出し可能な媒体におけるプログラムコードと、
前記第１環境信号と前記第２環境信号を合成しコンポジットセンサ信号にするための、前記コンピュータ読み出し可能な媒体におけるプログラムコードと、
前記コンポジットセンサ信号を、前記無線装置内の状況推定エンジンによって処理するための、前記コンピュータ読み出し可能な媒体におけるプログラムコードと、
前記状況推定エンジンにより処理された現在の状況に関する結果を出力するための、前記コンピュータ読み出し可能な媒体におけるプログラムコードと、
前記現在の状況に関する結果に応答し、前記ユーザーに情報を提供するための、前記コンピュータ読み出し可能な媒体におけるプログラムコードと、

を有するコンピュータプログラムプロダクト。

【請求項４８】

無線装置が、該装置の現在の環境に関連する情報をそのユーザーに提供できるようにする方法であって、

限定された処理能力と記憶容量を有する、前記無線装置の現在の環境を特徴付けるセンサ信号を受信するステップと、

高度演算負荷（computationally intensive load）と記憶の条件により特徴付けられる状況推定処理により、前記センサ信号を処理するステップと、

前記状況推定処理が前記無線装置内の第１状況推定エンジンにより部分的に実行され、部分的に処理されたセンサ信号を生成するステップと、

前記部分的に処理されたセンサ信号を、別個のネットワークサーバー内の第２状況推定エンジンに送信し、高度演算負荷の一部を、前記無線装置からサーバに負荷分散するステップと、

前記状況推定処理が第２状況推定エンジンにより完了し、現在の状況に関する結果を生成するステップと、

前記現在の状況に関する結果に応答し、前記ユーザーに情報を提供するステップと、

を有する方法。